VORLESUNGEN

ÜBER

ZAHLENTHEORIE

VON

P. G. LEJEUNE DIRICHLET.

VORLESUNGEN

ÜBER

ZAHLENTHEORIE

VON

P. G. LEJEUNE DIRICHLET.

HERAUSGEGEBEN

UND

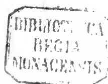
MIT ZUSÄTZEN VERSEHEN

VON

R. DEDEKIND,
Professor der höheren Mathematik am Collegium Carolinum zu Braunschweig.

ZWEITE
UMGEARBEITETE UND VERMEHRTE AUFLAGE.

BRAUNSCHWEIG,
DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN.
1871.


BIBLIOTHECA
REGIA
MONACENSIS

VORWORT DES HERAUSGEBERS.

Gleich nach dem Tode *Dirichlet's* wurde ich mehrfach aufgefordert, die von ihm gehaltenen Universitäts-Vorlesungen, welche so ausserordentlich viel zur Verbreitung der Bekanntschaft mit neueren und feineren Theilen der Mathematik beigetragen haben, in möglichst getreuer Form zu veröffentlichen; ich glaubte dieser Aufforderung um so eher nachkommen zu können, als ich in den Jahren 1855 bis 1858 die wichtigsten dieser Vorlesungen in Göttingen gehört und ausserdem vielfach Gelegenheit gehabt hatte, im persönlichen Verkehr *Dirichlet's* Gründe für die von ihm befolgte Methode des Vortrags kennen zu lernen. Nachdem auch die Verwandten *Dirichlet's* mich dazu ermächtigt haben, so übergebe ich dem mathematischen Publicum hiermit eine Ausarbeitung der Vorlesung über Zahlentheorie, bei welcher im Wesentlichen der im Winter 1856 bis 1857 von *Dirichlet* befolgte Gang eingehalten ist; er selbst fasste damals den Gedanken einer Herausgabe dieser Vorlesungen, und da er seinen

Vortrag nie schriftlich ausgearbeitet hatte, so diente ihm ein von mir geschriebenes, allerdings nur die Hauptmomente der Beweise enthaltendes Heft dazu, einen ungefähren Ueberschlag über die Ausdehnung der einzelnen Abschnitte zu machen. In öfter wiederkehrenden Gesprächen über diesen Plan äusserte er die Absicht, bei der Veröffentlichung manche Abschnitte hinzufügen zu wollen, die in einem Lehrbuch nicht fehlen dürften, die aber in jener Wintervorlesung aus Mangel an Zeit übergangen werden mussten. Bei der jetzigen Herausgabe ist daher im Wesentlichen zwar das eben erwähnte Heft zu Grunde gelegt, aber ich habe theils nach älteren Heften, theils nach *Dirichlet'schen* Abhandlungen, endlich auch ganz nach eigenem Ermessen Zusätze von nicht unbedeutender Ausdehnung gemacht, welche ich hier anführen zu müssen glaube, um für sie die Verantwortlichkeit zu übernehmen; sie sind in den Paragraphen 105 bis 110, 121 bis 144 und in den unmittelbar unter den Text gesetzten Anmerkungen enthalten.

Es ist meine Absicht, diesem ersten Bande, dessen Vollendung durch andere Arbeiten sich bis jetzt verzögert hat, zunächst einen zweiten weniger umfangreichen nachfolgen zu lassen, in welchem die Vorlesung über die im umgekehrten Verhältniss des Quadrats der Entfernung wirkenden Kräfte wiedergegeben werden soll.

Braunschweig, im October 1863.

R. Dedekind.

VORWORT ZUR ZWEITEN AUFLAGE.

Diese neue Auflage unterscheidet sich von der ersten hauptsächlich dadurch, dass sie um das zehnte Supplement bereichert ist, welches von der Composition der Formen handelt. Dieser Gegenstand war bei der ersten Auflage gänzlich ausgeschlossen geblieben, weil die einzige Abhandlung *Dirichlet's*, welche sich unmittelbar hierauf bezieht, nur den ersten Fundamentalsatz behandelt, weshalb ich befürchten musste, bei einer vollständigen Darstellung dieser Theorie mich zu weit von dem ursprünglichen Zwecke der Herausgabe zu entfernen. Obwohl ich nun diese Gefahr auch jetzt durchaus nicht verkenne, so habe ich mich doch aus vielen Gründen entschlossen, das zehnte Supplement hinzuzufügen und dadurch mehrfachen an mich gerichteten Aufforderungen nach besten Kräften zu entsprechen, hauptsächlich, weil trotz des ungemeinen Interesses und der steigenden Wichtigkeit dieser Theorie noch immer kein Versuch gemacht ist, die grossen Schwierigkeiten hinwegzuräumen, welche beim Eindringen

in dieselbe sich dem Anfänger entgegenstellen, und weil die übrigen Abschnitte des Werkes ganz vorzüglich geeignet sind, einen solchen Versuch zu erleichtern. Bei der wirklichen Ausführung dieses Entschlusses habe ich mich nicht auf die Begründung der ersten Elemente beschränkt, sondern es für nothwendig gehalten, den grössten Theil der in der fünften Section der *Disquisitiones Arithmeticae* enthaltenen Untersuchungen möglichst kurz und einfach zur Darstellung zu bringen. Endlich habe ich in dieses Supplement eine allgemeine Theorie der *Ideale* aufgenommen, um auf den Hauptgegenstand des ganzen Buches von einem höheren Standpuncte aus ein neues Licht zu werfen; hierbei habe ich mich freilich auf die Darstellung der Grundlagen beschränken müssen, doch hoffe ich, dass das Streben nach charakteristischen Grundbegriffen, welches in anderen Theilen der Mathematik mit so schönen Erfolgen gekrönt ist, mir nicht ganz missglückt sein möge. Die Untersuchungen in diesem von *Kummer* geschaffenen Gebiete, welche *Kronecker* vor vierzehn Jahren angestellt hat, sind bis jetzt nicht veröffentlicht, und ich vermag nach den damaligen brieflichen Mittheilungen dieses ausgezeichneten Mathematikers nicht zu beurtheilen, in welchen Beziehungen seine Principien zu den meinigen stehen. Der Aufbau der Theorie in §. 163 befriedigt mich selbst zwar noch nicht vollständig; allein es ist mir erst nach sehr langem Nachdenken geglückt, ihm diese Form zu geben, während ich vor etwa zehn Jahren von der Theorie der höheren Congruenzen in Verbindung mit den Principien von *Galois* zu einer ganz anderen Begründungsart gelangt war, welche einige

Berührungspuncte mit der Theorie der idealen Zahlen von *Selling* hat, mir aber jetzt weniger naturgemäss erscheint. Eine ausführlichere Darstellung der an den Begriff eines *Körpers* (§. 159) sich anschliessenden algebraischen Principien, welche hier nur beiläufig angedeutet werden konnten, verspare ich mir für eine andere Gelegenheit.

Es ist natürlich, dass die Hinzufügung des zehnten Supplementes einige Rückwirkung auf die früheren Abschnitte ausgeübt hat; doch braucht man nicht zu besorgen, dass ich mich durch solche Abänderungen der ersten Auflage im Plan und in der Haltung der Darstellung von der eigentlichen Grundlage, den Vorlesungen *Dirichlet's*, weiter entfernt habe. Um einem etwaigen Vorwurfe dieser Art von vornherein zu begegnen, wiederhole ich hier (aus den Göttinger Gelehrten Anzeigen vom 27. Januar 1864), dass auch die erste Auflage sich nicht auf ein in den Vorlesungen selbst nachgeschriebenes Heft, sondern nur auf Notizen stützt, welche ich aus der Erinnerung und grösstentheils in äusserst kurzer Form verfasst habe; als ich diese Vorlesungen als Privatdocent in Göttingen hörte, war ich mit dem Stoffe hinreichend vertraut, und mein Hauptzweck bestand darin, den überaus eindringlichen Vortrag *Dirichlet's* vollständig auf mich wirken zu lassen. Bei der Herausgabe der ersten Auflage, welche erst nach einer Reihe von Jahren erfolgte, wurde es nothwendig, diese Notizen ganz neu auszuarbeiten und auch durch eigene Zuthaten (z. B. §. 2, wenn ich nicht irre) zu ergänzen, die unmöglich alle erwähnt werden konnten. Aber damals sowohl wie jetzt

ist es mein eifrigstes Streben gewesen, *Dirichlet's* Vortrag mit grösster Treue wiederzugeben. Volle Freiheit habe ich mir dagegen bei den eigenen Zusätzen gestattet; gänzlich umgearbeitet sind z. B. die §§. 105 bis 110, 143, 144, und manches Neue ist theils im Text, theils in Form von Noten hinzugefügt.

Endlich habe ich mich bemüht, überall, wo es mir möglich war, auf die Quellen zu verweisen, um den Leser zum Studium der Originalwerke zu veranlassen und in ihm ein Bild von den Fortschritten der Wissenschaft zu erwecken, deren ebenso tiefe wie erhabene Wahrheiten einen Schatz bilden, welcher die unvergängliche Frucht eines wahrhaft edelen Wettkampfes der europäischen Völker ist.

Braunschweig, 1. März 1871.

R. Dedekind.

INHALT.

Seite

Erster Abschnitt: Von der Theilbarkeit der Zahlen.

Seite

Zweiter Abschnitt: Von der Congruenz der Zahlen.

Dritter Abschnitt: Von den quadratischen Resten.

Supplemente.

Erster Abschnitt.

Von der Theilbarkeit der Zahlen.

§. 1.

Wir behandeln in diesem Abschnitte einige arithmetische Sätze, welche man zwar in den meisten Lehrbüchern vorfindet, die aber für unsere Wissenschaft von so fundamentaler Bedeutung sind, dass eine strenge Begründung derselben hier durchaus nothwendig erscheint. Dahin gehört zuerst der Satz, dass das Product einer Reihe von ganzen positiven Zahlen unabhängig von der Anordnung ist, in welcher man die Multiplication ausführt. Indem wir uns zunächst auf den Fall beschränken, in welchem es sich um *drei* Zahlen a, b, c handelt, bilden wir das folgende Schema

$$\begin{array}{l} c,\ c,\ c,\ c \ldots c \\ c,\ c,\ c,\ c \ldots c \\ c,\ c,\ c,\ c \ldots c \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ c,\ c,\ c,\ c \ldots c \end{array}$$

welches aus b Horizontalreihen besteht, deren jede die Zahl c gleich oft, nämlich $a$mal enthält, und stellen uns die Aufgabe, die Summe aller aufgeschriebenen Zahlen zu bestimmen. Zunächst können wir sagen: da die Zahl c in jeder Horizontalreihe $a$mal vorkommt, so ist nach dem Grundbegriff der Multiplication die

Summe aller in einer solchen Reihe befindlichen Zahlen gleich ca, indem wir den *Multiplicand* c durch die Stellung von dem *Multiplicator* a unterscheiden; da ferner b solche Horizontalreihen vorhanden sind, so ist die Summe sämmtlicher Zahlen gleich $(ca)b$, wo jetzt ca der Multiplicand, b der Multiplicator ist. Nun können wir aber dieselbe Summe auch auf anderm Wege durch die Bemerkung bestimmen, dass das obige Schema aus a Verticalreihen besteht, deren jede b mal die Zahl c enthält; es ist also die Summe aller in einer Verticalreihe befindlichen Zahlen gleich cb, und folglich die Totalsumme gleich $(cb)a$. Wir erhalten mithin das erste Resultat

$$(ca)b = (cb)a,$$

aus welchem wir, indem wir die bisher ganz willkürliche Zahl $c = 1$ setzen, die Folgerung ziehen, dass

$$ab = ba$$

ist, d. h.: *in einem Product aus zwei ganzen positiven Zahlen dürfen Multiplicand und Multiplicator mit einander vertauscht werden.* Man lässt deshalb auch in der Benennung den Unterschied zwischen Multiplicand und Multiplicator ganz fallen, indem man beide unter dem gemeinschaftlichen Namen *Factoren* zusammenfasst.

Wir können nun dieselbe Totalsumme sämmtlicher in dem obigen Schema befindlichen Zahlen noch auf eine dritte Art bestimmen, indem wir abzählen, wie oft der Summand c im Ganzen vorkommt. Zunächst ist a die Anzahl der in einer jeden Horizontalreihe befindlichen Zahlen c, und folglich ist, da b solche Horizontalreihen vorhanden sind, die Anzahl aller aufgeschriebenen Zahlen gleich ab. Hieraus folgt, dass die Totalsumme den Werth $c(ab)$ hat, dass also

$$(ca)b = (cb)a = c(ab)$$

ist. Verbindet man hiermit den schon oben betrachteten speciellen Fall $ab = ba$, so kann man das Bisherige in folgendem Satze zusammenfassen:

Wenn man von drei positiven ganzen Zahlen zwei nach Belieben auswählt und als Factoren zu ihrem Producte vereinigt, sodann dieses Product und die dritte jener drei Zahlen mit einander multiplicirt, so hat das so entstehende Product stets denselben Werth, wie man auch die ersten beiden Zahlen ausgewählt haben mag.

Da also dieses Product von der Anordnung der beiden successiven Multiplicationen ganz unabhängig ist, so bezeichnet man

dasselbe kurz als das Product aus jenen drei Zahlen und nennt diese letzteren ohne Unterschied die Factoren des Productes.

§. 2.

Es ist nun leicht zu zeigen, ohne ein neues Princip anzuwenden, dass ein ganz ähnlicher allgemeinerer Satz für jedes System S von beliebig vielen positiven ganzen Zahlen

$$a, b, c \ldots$$

gilt. Die allgemeinste Art, diese Zahlen durch wiederholte Anwendung einfacher, d. h. auf nur zwei Zahlen bezüglicher Multiplicationen zu einem Producte zu vereinigen, ist folgende. Man greife nach Belieben zwei Zahlen aus dem System S heraus und bilde ihr Product; der aus den übrigen Zahlen des Systems S und aus diesem Product bestehende Zahlencomplex S' enthält dann eine Zahl weniger als S; indem man wieder ganz nach Belieben zwei Zahlen aus S' zu ihrem Producte vereinigt und die anderen unverändert lässt, erhält man ein System S'' von Zahlen, deren Anzahl um zwei kleiner ist als die der ursprünglich gegebenen Zahlen. Fährt man so fort, so wird man zuletzt zu einer einzigen Zahl gelangen, und der zu beweisende Satz besteht darin, *dass diese am Ende des Processes resultirende Zahl immer dieselbe sein wird, auf welche Art man auch die einzelnen einfachen Multiplicationen anordnen mag.*

Um dies zu zeigen, wenden wir die vollständige Induction an, d. h. wir nehmen an, der Satz sei richtig, wenn die Anzahl der ursprünglich gegebenen Zahlen oder Factoren $= n$ ist, und beweisen, dass er dann auch für die nächst grössere Anzahl $n + 1$ von Factoren ebenfalls gültig sein muss. Es sei also ein System S von $n + 1$ Zahlen

$$a, b, c, d, e \ldots$$

gegeben, so wähle man irgend zwei derselben, z. B. a und b, und bilde ihr Product ab; der nun entstehende Zahlencomplex enthält nur noch die n Zahlen

$$ab, c, d, e \ldots$$

und folglich ist nach unserer Annahme das Endresultat von der weitern Anordnung des Processes ganz unabhängig. Bei einer andern Anordnung der ganzen Operation kann daher höchstens

dann ein anderes Endresultat zum Vorschein kommen, wenn das bei dem ersten Schritte ausgewählte Zahlenpaar von a, b verschieden ist, und zwar sind zwei Fälle zu unterscheiden.

Erstens kann es sein, dass bei der zweiten Anordnung zuerst *eine* der beiden Zahlen a, b, z. B. a, mit einer der übrigen c, d, e . . ., z. B. mit c, zu dem Producte ac vereinigt wird, so dass der nächste Complex aus den n Zahlen

$$ac, b, d, e \ldots$$

besteht; da nun sowohl bei der erstern wie bei der letztern Anordnung die auf den ersten Schritt folgenden Operationen keinen Einfluss auf das Endresultat ausüben können, so setze man die erste Anordnung so fort, dass zunächst die beiden Zahlen ab und c, die zweite so, dass zunächst die beiden Zahlen ac und b vereinigt werden. Auf diese Weise entsteht bei der ersten Anordnung zunächst der Complex

$$(ab)c, d, e \ldots$$

bei der zweiten der Complex

$$(ac)b, d, e \ldots$$

Da nun zufolge des vorhergehenden Paragraphen die beiden Producte $(ab)c$ und $(ac)b$ und folglich auch die beiden vorstehenden Complexe identisch sind, so wird, da jeder derselben nur noch $n-1$ Zahlen enthält, bei der ersten wie bei der zweiten Anordnung dasselbe Endresultat auftreten.

Zweitens kann es aber auch sein, dass bei dem ersten Schritt der zweiten Anordnung *keine* der beiden Zahlen a, b, sondern zwei von den übrigen, z. B. c, d, herausgegriffen werden, so dass zunächst der Complex

$$a, b, cd, e \ldots$$

entsteht. Auch jetzt kann man wieder die auf den ersten Schritt folgenden Operationen bei beiden Anordnungen nach Belieben ausführen; man vereinige daher zunächst bei der ersten Anordnung die Zahlen c, d, und bei der zweiten Anordnung die Zahlen a, b; dann besteht bei beiden Anordnungen der nächstfolgende Complex aus denselben $n-1$ Zahlen

$$ab, cd, e \ldots$$

und folglich wird abermals das Endresultat bei beiden dasselbe sein.

Hiermit ist die Allgemeingültigkeit des Satzes bewiesen; denn da er nach dem vorhergehenden Paragraphen für $n = 3$ gilt, so

gilt er nach dem Vorstehenden auch für alle Systeme von Zahlen, deren Anzahl = 4, 5, 6 u. s. w. ist. Das Endresultat heisst auch jetzt wieder das Product aus den gegebenen Zahlen, diese letzteren heissen die Factoren des Productes, und man bezeichnet das Product durch das Nebeneinanderschreiben sämmtlicher in beliebiger Ordnung folgenden Factoren.

Ein besonderer Fall dieses Satzes ist der, dass man bei der Bildung des Productes aus beliebig vielen Zahlen oder Factoren dieselben nach Belieben in Gruppen vertheilen und alle in einer Gruppe enthaltenen Factoren zu ihrem Product vereinigen darf; das Product aus diesen den einzelnen Gruppen entsprechenden Producten wird immer mit dem Producte aller gegebenen Zahlen übereinstimmen; denn offenbar ist diese Bildung selbst eine der verschiedenen möglichen Anordnungen des Processes. So ist z. B.

$$abcde = (ab)c(de) = (abcd)e = (abe)(cd).$$

Es ist nicht schwierig, dieselben Sätze auch für den Fall zu beweisen, dass unter den Factoren eines Productes beliebig viele *negative* sind; das Vorzeichen des Productes wird das positive oder negative sein, je nachdem die Anzahl der negativen Factoren gerade oder ungerade ist. Endlich mag noch daran erinnert werden, dass auch die ganze Zahl *Null* als Factor auftreten kann, in welchem Falle das Product stets = 0 sein wird.

§. 3.

Wenn die Zahl*) a das Product aus der Zahl b und einer zweiten ganzen Zahl m, also $a = mb$ ist, so nennt man a ein *Vielfaches* oder *Multiplum* von b; statt dessen sagt man auch: a ist *theilbar* durch b, oder: b ist ein *Theiler* oder *Divisor* von a, oder endlich: *b geht in a auf.* Alle diese Benennungen sind gleich gebräuchlich, und da es in der Zahlentheorie ausserordentlich oft vorkommt, diese Beziehung zwischen zwei Zahlen auszudrücken, so ist es angenehm, dafür eine Reihe verschiedener Ausdrücke zu besitzen. Aus der Definition des Vielfachen leuchten nun sogleich folgende Sätze ein, von denen später sehr häufig Gebrauch gemacht werden wird.

*) Unter *Zahlen* schlechthin sind hier und im Folgenden immer *ganze* Zahlen zu verstehen.

1. Ist a Multiplum von b, b wieder Multiplum von c, so ist auch a Multiplum von c. Denn der Annahme nach ist $a = mb$, $b = nc$, wo m und n irgend zwei ganze Zahlen bedeuten; hieraus folgt $a = m(nc) = (mn)c$, also ist a theilbar durch c.

Allgemein: hat man eine Reihe von Zahlen, in welcher jede ein Vielfaches der nächstfolgenden ist, so ist auch jede frühere Zahl ein Vielfaches von jeder spätern.

2. Ist die Zahl a sowohl als auch b ein Multiplum einer dritten Zahl c, so ist auch die Summe und die Differenz der beiden ersteren ein Multiplum der dritten. Denn aus $a = mc$, $b = nc$ folgt $a \pm b = (m \pm n)c$.

§. 4.

Von der grössten Wichtigkeit für die Lehre von der Theilbarkeit der Zahlen ist folgende Aufgabe *): *Wenn irgend zwei ganze positive Zahlen a, b gegeben sind, so sollen die gemeinschaftlichen Theiler derselben, d. h. diejenigen Zahlen δ gefunden werden, welche gleichzeitig in a und in b aufgehen.*

Wir können annehmen, es sei a grösser oder wenigstens nicht kleiner als b; dann wird die Division von a durch b einen Quotienten m und einen Rest c geben, welcher letztere jedenfalls kleiner als b ist. Betrachten wir nun die aus dieser Division resultirende Gleichung

$$a = mb + c$$

und nehmen wir an, es sei δ irgend eine sowohl in a als in b aufgehende Zahl, so ist δ jedenfalls auch ein Divisor des Restes c; denn da a und b Multipla von δ sind, so ist (nach §. 3) mb, und folglich auch die Differenz $a - mb = c$ ein Multiplum von δ. Wir können daher sagen: jeder gemeinschaftliche Theiler der beiden Zahlen a, b ist auch ein gemeinschaftlicher Theiler der beiden Zahlen b, c. Umgekehrt, ist δ ein gemeinschaftlicher Divisor der beiden Zahlen b, c, so ist, da δ dann auch in mb aufgeht, die Summe $mb + c = a$ der beiden Multipla mb und c von δ ebenfalls ein Multiplum von δ; also ist jeder gemeinschaftliche Divisor der Zahlen b, c auch gemeinschaftlicher Divisor der Zahlen a, b. Mithin stimmen die gemeinschaftlichen Divisoren der beiden Zahlen a, b

*) *Euclid's Elemente*, Buch VII, Satz 2.

vollständig mit denen der beiden Zahlen b, c überein; unsere Untersuchung ist daher von dem Paare a, b auf das Paar b, c reducirt, und da b nicht grösser als a, c aber jedenfalls kleiner als b ist, so können wir mit Recht sagen, dass das Problem auf ein einfacheres zurückgeführt sei.

Wenn nun c von Null verschieden ist, die erste Division also nicht aufgeht, so können wir, indem wir b durch die kleinere Zahl c dividiren, wieder eine Gleichung von der Form

$$b = nc + d$$

bilden, in welcher der Divisionsrest d kleiner als der vorhergehende c ist. Durch eine der obigen ganz ähnliche Betrachtung ergiebt sich dann, dass die gemeinschaftlichen Divisoren der beiden Zahlen c, d vollständig mit denen der Zahlen b, c und also auch mit denen der Zahlen a, b übereinstimmen.

So kann man fortfahren, bis einmal die Division aufgeht, was nach einer endlichen Anzahl von Operationen durchaus eintreten muss; denn die Zahlen $b, c, d \ldots$ bilden eine Reihe von beständig abnehmenden Zahlen, und da es nur eine endliche Anzahl von Zahlen giebt, welche kleiner sind als b, so muss unter ihnen endlich auch die Null erscheinen. Wir haben dann eine Kette von Gleichungen von der Form

$$\begin{aligned} a &= mb + c \\ b &= nc + d \\ c &= pd + e \\ &\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots \\ f &= sg + h \\ g &= th. \end{aligned}$$

Jeder gemeinschaftliche Divisor δ von a, b ist auch Divisor der folgenden Zahlen $c, d \ldots$, endlich auch von h; umgekehrt, ist δ ein Divisor von h, so lehrt die letzte Gleichung, dass δ auch Divisor von g, also gemeinschaftlicher Divisor von g und h ist; folglich ist δ auch Divisor von f und ebenso von den vorhergehenden Zahlen, endlich auch von b und von a. Wir haben daher das Resultat:

Die gemeinschaftlichen Divisoren zweier Zahlen a und b stimmen überein mit den sämmtlichen Divisoren Einer bestimmten Zahl h, welche man durch den obigen Algorithmus stets finden kann. Da nun h selbst zu diesen Divisoren gehört und unter ihnen dem

Werth nach der grösste ist, so nennt man diese Zahl h den *grössten gemeinschaftlichen Divisor* der beiden Zahlen a und b.

Hiermit ist nun zwar unser Problem nicht vollständig gelöst, sondern nur auf das andere zurückgeführt, sämmtliche Divisoren einer gegebenen Zahl h zu finden, für welches wir noch keine directe Lösung haben; allein es wird sich im Folgenden hinreichend zeigen, dass der obige Algorithmus ein Fundament bildet, auf welchem sich die Grundprincipien der Zahlentheorie mit ebenso grosser Strenge wie Leichtigkeit aufbauen lassen. Nur einige Bemerkungen noch, um auch nicht den geringsten Zweifel gegen die Allgemeinheit der folgenden Sätze aufkommen zu lassen: wir haben die obige Kette von Gleichungen gebildet unter der Voraussetzung, dass a nicht kleiner als b sei; allein für den Fall, dass $a < b$ sein sollte, braucht man nur $m = 0$, also $c = a$ zu nehmen, um dieselbe Form auch dann zu wahren. Ebenso leicht erkennt man, dass das Vorzeichen der Zahlen a, b ganz unwesentlich ist; ja, es darf sogar eine von ihnen $= 0$ sein; nur, wenn beide $= 0$ sind, kann von einem grössten gemeinschaftlichen Divisor derselben keine Rede sein.

§. 5.

Besonders interessant ist der specielle Fall, in welchem der grösste gemeinschaftliche Divisor zweier Zahlen a, b die Einheit ist; man nennt zwei solche Zahlen *relative Primzahlen*, auch wohl *Zahlen ohne gemeinschaftlichen Divisor*, indem man absieht von dem allen Zahlen gemeinschaftlichen Divisor 1; oder man sagt auch: a ist relative Primzahl *gegen* oder *zu* b. Dieser Definition zufolge erkennt man also zwei Zahlen als relative Primzahlen daran, dass bei dem Algorithmus des grössten gemeinschaftlichen Divisors einmal der Rest $h = 1$ auftritt. Für solche Zahlen gilt nun der folgende

Hauptsatz: Sind a, b relative Primzahlen, und ist k eine beliebige dritte Zahl, so ist jeder gemeinschaftliche Theiler der beiden Zahlen ak, b auch gemeinschaftlicher Theiler der beiden Zahlen k, b.

Um sich hiervon zu überzeugen, braucht man nur sämmtliche Gleichungen, die bei dem Algorithmus des grössten gemeinschaftlichen Divisors der Zahlen a, b gebildet werden, und deren vorletzte, da $h = 1$ ist, in unserm Falle $f = sg + 1$ lautet, mit k zu multipliciren; man erhält dann

$$ak = mbk + ck$$
$$bk = nck + dk$$
$$ck = pdk + ek$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$fk = sgk + k.$$

Ist nun δ irgend ein gemeinschaftlicher Divisor von ak und b, so geht δ auch in mbk, also auch in $ak - mbk = ek$ auf; es geht daher δ auch in nck und folglich auch in $bk - nck = dk$ auf. Und indem man diese Schlussweise fortsetzt, gelangt man zu dem Resultat, dass δ auch in fk, in gk, folglich auch in $fk - sgk = k$ aufgehen muss, was zu beweisen war.

Im Folgenden werden wir vorzüglich zwei specielle Fälle dieses Satzes gebrauchen, nämlich:

1. *Das Product zweier Zahlen a und k, deren jede relative Primzahl gegen eine dritte b ist, ist gleichfalls relative Primzahl zu b;* denn unserm Satze nach haben ak und b dieselben gemeinschaftlichen Divisoren, wie k und b; da aber k und b relative Primzahlen sind, so haben sie nur den einzigen gemeinschaftlichen Divisor 1; dasselbe gilt daher von ak und b, also sind diese Zahlen relative Primzahlen.

2. *Sind a und b relative Primzahlen, und ist ak durch b theilbar, so ist auch k durch b theilbar;* denn da der Annahme zufolge ak und b den gemeinschaftlichen Divisor b haben, so muss dem Hauptsatze nach b auch gemeinschaftlicher Divisor von k und b, also jedenfalls Divisor von k sein.

3. Den ersten dieser beiden Sätze kann man leicht verallgemeinern. Ist jede der Zahlen $a, b, c, d \ldots$ relative Primzahl gegen eine Zahl α, so ist auch ab, folglich auch das Product abc aus ab und c, folglich auch das Product $abcd$ aus abc und d u.s.f., kurz das Product $abcd \ldots$ aller jener Zahlen ebenfalls relative Primzahl gegen α. Allgemeiner, *hat man zwei Reihen von Zahlen*

$$a, b, c, d \ldots$$

und

$$\alpha, \beta, \gamma \ldots$$

von der Beschaffenheit, dass jede Zahl der einen Reihe relative Primzahl gegen jede Zahl der andern Reihe ist, so ist auch das Product $abcd \ldots$ aller Zahlen der einen Reihe relative Primzahl

gegen das Product $\alpha\beta\gamma$ ... aller Zahlen der andern Reihe. Denn soeben ist bewiesen, dass jede der Zahlen α, β, γ ... relative Primzahl gegen das Product $abcd$ ... ist, woraus durch nochmalige Anwendung desselben Satzes auch folgt, dass ihr Product $\alpha\beta\gamma$... ebenfalls relative Primzahl gegen $abcd$ ... ist.

4. Hieraus können wir wieder einen speciellen Fall ableiten, indem wir annehmen, dass die Zahlen b, c, d ... identisch mit a, ferner die Zahlen β, γ ... identisch mit α sind; wir erhalten dann das Resultat: *ist a relative Primzahl gegen α, so ist auch jede Potenz der Zahl a relative Primzahl gegen jede Potenz der Zahl α.*

Eine Anwendung hiervon macht man bei dem Beweise des Satzes, dass die $m$te Wurzel aus einer ganzen Zahl A entweder irrational oder selbst eine ganze Zahl ist; denn wenn jene Wurzel rational, d. h. von der Form $r:s$ ist, wo r und s ganze Zahlen bedeuten, die man ohne gemeinschaftlichen Divisor annehmen kann, so ergiebt sich aus $r^m = A s^m$, dass r^m durch s^m theilbar ist; da nun r und s, folglich auch r^m und s^m relative Primzahlen sind, so muss $s^m = 1$, also auch $s = 1$ sein; mithin ist jene Wurzel eine ganze Zahl r.

§. 6.

Die Aufgabe des §. 4 in der Weise verallgemeinert, dass für eine ganze Reihe gegebener Zahlen a, b, c, d ... alle gemeinschaftlichen Divisoren gesucht werden, führt zu einem ganz ähnlichen Resultate. Es sei h der grösste gemeinschaftliche Divisor von a und b, so ist, wie wir früher fanden, jeder gemeinschaftliche Divisor von a und b auch Divisor von h und umgekehrt; jeder gemeinschaftliche Divisor der drei Zahlen a, b, c ist daher auch gemeinschaftlicher Divisor von h, c und umgekehrt; bezeichnet man daher mit k den grössten gemeinschaftlichen Divisor von h und c, so ist jede gleichzeitig in a, b, c aufgehende Zahl Divisor von k, und umgekehrt wird jeder Divisor von k auch Divisor der drei Zahlen a, b, c sein. Bildet man ferner den grössten gemeinschaftlichen Divisor l der beiden Zahlen k und d, so stimmen die gemeinschaftlichen Divisoren der vier Zahlen a, b, c, d vollständig überein mit den sämmtlichen Divisoren der Zahl l u. s. f. Wir haben daher das Resultat: *ist irgend eine Reihe von Zahlen a, b, c, d ... gegeben, so giebt es stets eine — und natürlich auch nur*

eine — Zahl m *von der Beschaffenheit, dass jede gleichzeitig in* a, *in* b, *in* c, *in* d *u. s. w. aufgehende Zahl auch in* m *aufgeht, und umgekehrt jeder Divisor von* m *auch Divisor jeder einzelnen der Zahlen* $a, b, c, d \ldots$ *ist.* Diese vollkommen bestimmte Zahl m heisst deshalb wieder der *grösste gemeinschaftliche Divisor* der gegebenen Zahlen. (Eine Ausnahme hiervon tritt nur dann ein, wenn die gegebenen Zahlen *alle* $= 0$ sind.) Setzt man ferner $a = ma'$, $b = mb'$, $c = mc'$, $d = md' \ldots$, so sind $a', b', c', d' \ldots$ ganze Zahlen, deren grösster gemeinschaftlicher Theiler $= 1$ ist, oder, wie man kurz sagt, *Zahlen ohne gemeinschaftlichen Theiler.* Umgekehrt, wenn $a', b', c', d' \ldots$ Zahlen ohne gemeinschaftlichen Theiler sind, so leuchtet ein, dass m der grösste gemeinschaftliche Theiler der Zahlen $ma', mb', mc', md' \ldots$ ist.

Dagegen bemerken wir an dieser Stelle ein- für allemal, dass, wenn Zahlen $a, b, c, d \ldots$ *relative Primzahlen* genannt werden, darunter stets zu verstehen ist, dass *je zwei* von ihnen relative Primzahlen sind; solche Zahlen sind daher stets zugleich Zahlen ohne gemeinschaftlichen Theiler; aber Zahlen ohne gemeinschaftlichen Theiler sind nicht nothwendig relative Primzahlen.

§. 7.

Gewissermaassen das Umgekehrte der vorhergehenden ist die folgende Aufgabe: *Wenn eine Reihe von Zahlen* $a, b, c, d \ldots$ *gegeben ist, so sollen alle gemeinschaftlichen Multipla derselben, d. h. alle Zahlen gefunden werden, welche durch jede einzelne der gegebenen Zahlen theilbar sind.* Da von den gesuchten Zahlen zuerst gefordert wird, dass sie durch a theilbar sein sollen, so sind sie jedenfalls in der Form sa enthalten, wo s irgend eine ganze Zahl bedeutet. Ist nun δ der grösste gemeinschaftliche Divisor der beiden Zahlen $a = \delta a'$ und $b = \delta b'$, so sind a' und b' relative Primzahlen; soll daher $sa = sa'\delta$ theilbar sein durch $b = b'\delta$, so muss sa' durch b' und folglich (§. 5, 2.) auch s durch b' theilbar, also von der Form $s'b'$ sein, wo s' wieder irgend eine ganze Zahl bedeutet. Sämmtliche sowohl durch a als durch b theilbare Zahlen sind daher von der Form $sa = s'.a'b'\delta$, und umgekehrt leuchtet ein, dass alle in dieser Form enthaltenen Zahlen sowohl durch $a = a'\delta$ als durch $b = b'\delta$ theilbar sind.

Es zeigt sich also, dass die sämmtlichen gemeinschaftlichen

Multipla der beiden Zahlen a, b übereinstimmen mit den sämmtlichen Vielfachen *einer* bestimmten Zahl

$$a' b' \delta = \frac{ab}{\delta} = \mu,$$

welche man deshalb das *kleinste gemeinschaftliche Vielfache* der beiden Zahlen a, b nennt.

Um diesen Satz für eine beliebige Anzahl gegebener Zahlen $a, b, c, d \ldots$ zu verallgemeinern, braucht man nur zu bemerken, dass jedes gemeinschaftliche Vielfache der Zahlen

$$a, b, c, d \ldots$$

nothwendig auch ein gemeinschaftliches Vielfaches der Zahlen

$$\mu, c, d \ldots$$

ist und umgekehrt. Man wird daher zunächst das kleinste gemeinschaftliche Multiplum ν der beiden Zahlen μ und c suchen, dann das kleinste gemeinschaftliche Vielfache ϱ von ν und d u. s. f. Auf diese Weise leuchtet ein, dass sämmtliche gemeinschaftliche Multipla der gegebenen Zahlen $a, b, c, d \ldots$ übereinstimmen mit den sämmtlichen Vielfachen einer einzigen vollständig bestimmten Zahl ω, welche man deshalb das *kleinste gemeinschaftliche Vielfache* der gegebenen Zahlen nennt.

Von besonderer Wichtigkeit ist der Fall, in welchem die Zahlen $a, b, c, d \ldots$ relative Primzahlen sind. In diesem Falle ist zunächst $\delta = 1$, also ist das kleinste gemeinschaftliche Vielfache der beiden relativen Primzahlen a und b ihr Product ab. Da nun c wieder relative Primzahl gegen a und gegen b, also (§. 5, 1.) auch gegen ab ist, so ist abc das kleinste gemeinschaftliche Multiplum der drei Zahlen a, b, c u. s. f. Kurz, man erhält das Resultat: *Sind $a, b, c, d \ldots$ relative Primzahlen, so ist jede Zahl, welche durch jede einzelne derselben theilbar ist, auch durch ihr Product $abcd \ldots$ theilbar.*

§. 8.

Da jede Zahl sowohl durch die Einheit, als auch durch sich selbst theilbar ist, so hat jede Zahl — die Einheit selbst ausgenommen — mindestens zwei (positive) Divisoren. Jede Zahl nun, welche keine anderen als diese beiden Divisoren besitzt, heisst eine *Primzahl (numerus primus)*; es ist zweckmässig, die Einheit nicht

zu den Primzahlen zu rechnen, weil manche Sätze über Primzahlen nicht für die Zahl 1 gültig bleiben.

Aus dieser Erklärung ergiebt sich der Satz: *Wenn p eine Primzahl und a irgend eine ganze Zahl ist, so geht entweder p in a auf, oder p ist relative Primzahl zu a.* Denn der grösste gemeinschaftliche Divisor von p und a ist entweder p selbst oder die Einheit.

Hieraus folgt weiter: *Wenn ein Product aus mehreren Zahlen $a, b, c, d \ldots$ durch eine Primzahl p theilbar ist, so geht p mindestens in einem der Factoren $a, b, c, d \ldots$ auf.* Denn wäre keine einzige dieser Zahlen durch p theilbar, so wäre p relative Primzahl gegen jede einzelne von ihnen und folglich auch gegen ihr Product, was gegen die Annahme streitet, dass dies Product durch p theilbar ist.

Jede Zahl, welche ausser sich selbst und der Einheit noch andere Divisoren hat, heisst *zusammengesetzt (numerus compositus).* Diese Benennung wird gerechtfertigt durch folgenden

Fundamentalsatz: Jede zusammengesetzte Zahl lässt sich stets und nur auf eine einzige Weise als Product aus einer endlichen Anzahl von Primzahlen darstellen.

Beweis. Da jede zusammengesetzte Zahl m ausser 1 und m noch andere Divisoren hat, so sei a ein solcher; ist nun a keine Primzahl, also eine zusammengesetzte Zahl, so besitzt a ausser 1 und a noch andere Divisoren, z. B. b; ist b noch keine Primzahl, also zusammengesetzt, so hat b wieder mindestens einen Divisor c, der von 1 und b verschieden ist. Fährt man so fort, so muss man endlich einmal zu einer Primzahl gelangen; denn die Reihe der Zahlen $m, a, b, c \ldots$ ist eine abnehmende, sie kann also, da es nur eine endliche Anzahl von Zahlen giebt, welche kleiner als m sind, nur eine endliche Anzahl von Gliedern enthalten; das letzte Glied derselben muss aber eine Primzahl sein, denn sonst könnte man ja die Reihe noch weiter fortsetzen. Bezeichnet man diese Primzahl mit p, so ist, da jedes Glied der Reihe ein Multiplum des folgenden ist, die erste Zahl m auch ein Multiplum von der letzten p. Man kann daher

$$m = pm'$$

setzen. Nun ist m' entweder eine Primzahl — dann ist m schon als Product von Primzahlen dargestellt — oder m' ist zusammengesetzt; im letztern Falle muss es wieder eine in m' aufgehende Primzahl p' geben, so dass

$$m' = p'm'', \quad \text{also} \quad m = pp'm''$$

wird. Ist nun m'' noch keine Primzahl, so kann man auf dieselbe Weise fortfahren, bis man m als Product von lauter Primzahlen dargestellt hat. Dass dies wirklich nach einer endlichen Anzahl von ähnlichen Zerlegungen geschehen muss, leuchtet daraus ein, dass die Reihe der Zahlen $m, m', m'' \ldots$ ebenfalls eine abnehmende und folglich eine endliche ist.

Hiermit ist der eine Haupttheil des Satzes erwiesen, welcher die Möglichkeit der Zerlegung behauptet; offenbar ist aber diese successive Ablösung von Primzahl-Factoren in mancher Beziehung willkürlich, und es bleibt daher noch nachzuweisen übrig, dass, auf welche Weise dieselbe auch ausgeführt sein mag, das Endresultat doch stets dasselbe sein muss. Nehmen wir daher an, man habe durch zwei verschiedene Anordnungen einmal

$$m = pp'p'' \ldots$$

ein anderes Mal

$$m = qq'q'' \ldots$$

gefunden, wo $p, p', p'' \ldots$ und $q, q', q'' \ldots$ sämmtlich Primzahlen bedeuten. Da nun das Product $pp'p'' \ldots$ durch die Primzahl q theilbar ist, so muss mindestens einer der Factoren, z. B. p, durch q theilbar sein; p besitzt aber als Primzahl nur die beiden Divisoren 1 und p, und folglich muss $q = p$ sein, da q nicht $= 1$ ist. Hieraus folgt nun

$$p'p'' \ldots = q'q'' \ldots$$

und man kann auf dieselbe Weise zeigen, dass q' mit einer der Primzahlen $p', p'' \ldots$, z. B. mit p', identisch sein muss, woraus dann wieder

$$p'' \ldots = q'' \ldots$$

folgt. Auf diese Weise überzeugt man sich davon, dass jede Primzahl, welche bei der zweiten Art der Zerlegung ein oder mehrere Male als Factor auftritt, mindestens ebenso oft auch bei der ersten Zerlegung vorkommt; da aber ferner auf dieselbe Weise gezeigt werden kann, dass sie bei der zweiten Zerlegung mindestens ebenso oft vorkommt wie bei der ersten, so muss jede Primzahl in beiden Zerlegungen gleich oft als Factor vorkommen, und folglich stimmt der Complex aller Primzahlen bei der einen Zerlegung vollständig mit dem bei der andern überein.

Nachdem so der Satz in allen seinen Theilen bewiesen ist,

können wir die Darstellung der zusammengesetzten Zahl m noch dadurch vereinfachen, dass wir jedesmal alle unter einander identischen Primzahl-Factoren zu einer Potenz vereinigen. Es sei nämlich a eine von den in m aufgehenden Primzahlen, und zwar mag dieselbe genau αmal als Factor in der Zerlegung vorkommen, so vereinigen wir diese α Factoren zu der Potenz a^α; sind hierdurch noch nicht alle Factoren erschöpft, und ist b eine der übrigen Primzahlen, so bilden wir, wenn sie genau βmal vorkommt, die Potenz b^β, und in derselben Weise fahren wir fort, wenn hierdurch noch nicht alle Primzahl-Factoren von m erschöpft sind. Auf diese Weise überzeugt man sich, dass man jeder zusammengesetzten Zahl m die Form

$$m = a^\alpha b^\beta c^\gamma \dots$$

geben kann, in welcher a, b, c die sämmtlichen unter einander verschiedenen, in m aufgehenden Primzahlen, und $\alpha, \beta, \gamma \dots$ ganze positive Zahlen bedeuten. Dass aber in dieser Form nicht nur alle zusammengesetzten, sondern auch alle Primzahlen enthalten sind, leuchtet unmittelbar ein.

Die Primzahlen bilden daher gewissermaassen das Material, aus welchem alle anderen Zahlen sich zusammensetzen lassen. *Dass es unendlich viele Primzahlen giebt*, hat schon *Euclid**) bewiesen, und zwar in folgender Art. Gesetzt es gäbe nur eine endliche Anzahl von Primzahlen, so würde eine von ihnen, die wir mit p bezeichnen wollen, die letzte, d. h. die grösste sein. Denken wir uns nun alle diese Primzahlen aufgeschrieben

$$2, 3, 5, 7, 11 \dots p,$$

so müsste jede Zahl, welche grösser als p ist, zusammengesetzt und folglich durch mindestens eine dieser Primzahlen theilbar sein. Allein es ist sehr leicht, eine Zahl zu bilden, welche erstens grösser als p und zweitens durch keine jener Primzahlen theilbar ist; dazu bilden wir das Product aller Primzahlen von 2 bis p und vergrössern dasselbe um eine Einheit. Diese Zahl

$$z = 2.\ 3.\ 5 \dots p + 1$$

ist in der That grösser als p, da ja schon $2p$ grösser als p ist; sie ist aber durch keine der Primzahlen theilbar, da z, durch jede derselben dividirt, immer den Rest 1 lässt. Damit ist also unsere

*) *Elemente*, Buch IX, Satz 20.

Annahme im Widerspruch, und folglich giebt es unendlich viele Primzahlen.

Dieser Satz ist nur ein specieller Fall des andern, dass in jeder unbegrenzten arithmetischen Progression, deren allgemeines Glied $kx + m$ ist, und in welcher das Anfangsglied m und die Differenz k relative Primzahlen sind, unendlich viele Primzahlen enthalten sind; allein, so einfach der Beweis für den speciellen Fall war, in welchem $k = 1$, so schwierig war es, einen strengen Beweis für den allgemeinen Satz zu geben, und dies ist bis jetzt nur durch Zuziehung von Principien gelungen, welche der Infinitesimalrechnung angehören *).

§. 9.

Durch den soeben bewiesenen Fundamentalsatz haben wir nun ein einfaches Kriterium gewonnen, nach welchem stets beurtheilt werden kann, ob eine Zahl m durch eine andere n theilbar ist oder nicht, sobald wir voraussetzen dürfen, dass beide in ihre Primfactoren zerlegt sind. Nehmen wir nämlich an, dass m durch n theilbar, dass also $m = nq$ ist, so leuchtet ein, dass jede in n aufgehende Primzahl auch in m aufgehen muss; es kann daher n keine anderen Primfactoren enthalten als m, und ausserdem kann auch ein solcher Primfactor nicht öfter in n als in m vorkommen; und umgekehrt, wenn jeder Primfactor der Zahl n mindestens ebenso oft in m vorkommt wie in n, so ist auch m durch n theilbar.

Sind daher a, b, c .. die sämmtlichen von einander verschiedenen, in m aufgehenden Primzahlen, so dass

$$m = a^{\alpha} b^{\beta} c^{\gamma} \ldots,$$

so ist jeder Divisor n dieser Zahl in der Form

$$n = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$$

enthalten, in welcher

α' irgend eine der $\alpha + 1$ Zahlen $0, 1, 2 \ldots \alpha$
β' „ „ „ $\beta + 1$ „ $0, 1, 2 \ldots \beta$
γ' „ „ „ $\gamma + 1$ „ $0, 1, 2 \ldots \gamma$
u. s. w.

*) Siehe die Supplemente VI. §. 132 bis 137.

bedeutet; und alle diese Zahlen n sind wirklich Divisoren von m. Hieraus gehen sogleich einige interessante Folgerungen hervor.

Zunächst leuchtet ein, da jede Combination eines Werthes von α' mit einem von β', mit einem von γ' u. s. w. einen Divisor von m liefert, und da je zwei verschiedenen solchen Combinationen (nach §. 8) auch zwei ungleiche Divisoren von m entsprechen, dass die Anzahl aller Divisoren von m gleich

$$(\alpha+1)\,(\beta+1)\,(\gamma+1)\ldots$$

ist; diese Anzahl hängt daher nur von den Exponenten $\alpha, \beta, \gamma \ldots$ ab, nicht aber von der Natur der in m aufgehenden Primzahlen a, b, c u. s. w.

Bildet man ferner das Schema

$$\begin{array}{l} 1,\ a,\ a^2 \ldots a^\alpha \\ 1,\ b,\ b^2 \ldots b^\beta \\ 1,\ c,\ c^2 \ldots c^\gamma \\ \quad\text{u. s. w.} \end{array}$$

und bildet alle Producte $a^{\alpha'}\, b^{\beta'}\, c^{\gamma'} \ldots$, indem man aus jeder dieser Horizontalreihen ein Glied $a^{\alpha'}, b^{\beta'}, c^{\gamma'} \ldots$ auswählt, so erhält man alle Divisoren der Zahl m, und zwar jeden nur ein einziges Mal. Die Summe aller dieser Divisoren erhält man daher nach derselben Regel, nach welcher man die einzelnen Aggregate

$$1+a+a^2+\ldots+a^\alpha = \frac{a^{\alpha+1}-1}{a-1}$$

$$1+b+b^2+\ldots+b^\beta = \frac{b^{\beta+1}-1}{b-1}$$

$$1+c+c^2+\ldots+c^\gamma = \frac{c^{\gamma+1}-1}{c-1}$$

u. s. w.

mit einander zu multipliciren hat; folglich ist die Summe aller Divisoren der Zahl m gleich dem Product

$$\frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \ldots$$

Nehmen wir z. B. $m = 60 = 2^2 . 3 . 5$, so sind die sämmtlichen Divisoren folgende:

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 30,\ 60;$$

ihre Anzahl ist

$$(2+1)\,(1+1)\,(1+1) = 12$$

und ihre Summe

$$\frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=7.4.6=168.$$

§. 10.

Wir kehren nun zu einigen früheren Aufgaben zurück, zunächst zu derjenigen (§. 6), den grössten gemeinschaftlichen Divisor einer Reihe von Zahlen zu bilden, jetzt unter der Voraussetzung, dass ihre Zerlegungen in Primfactoren gegeben sind. Man betrachte alle Primzahlen, welche in diesen Zerlegungen vorkommen, und scheide zunächst diejenigen unter ihnen aus, welche in einer oder mehreren der gegebenen Zahlen gar nicht als Primfactoren enthalten sind. Bleibt auf diese Weise gar keine Primzahl übrig, so ist die Einheit der gesuchte grösste gemeinschaftliche Divisor. Im entgegengesetzten Fall sei a eine Primzahl, welche bei dieser vorläufigen Ausscheidung zurückgeblieben ist und also in jeder der gegebenen Zahlen mindestens einmal enthalten ist; man zähle, wie oft a als Primfactor in jeder einzelnen der gegebenen Zahlen vorkommt, und nehme die kleinste dieser Anzahlen, die wir mit α bezeichnen, so dass a in mindestens einer der gegebenen Zahlen genau α mal, in allen übrigen aber mindestens ebenso oft als Primfactor vorkommt. Aehnlich verfahre man mit den übrigen Primzahlen $b, c \ldots$, sofern diese noch nicht erschöpft sind, und bilde für jede, für b die Anzahl β, für c die Anzahl γ u. s. w. nach derselben Regel, nach welcher für die Primzahl a die Anzahl α gebildet wurde. Dann ist

$$a^\alpha b^\beta c^\gamma \ldots$$

der gesuchte grösste gemeinschaftliche Divisor. Der Beweis für diese Regel leuchtet unmittelbar dadurch ein, dass der grösste gemeinschaftliche Divisor keine anderen Primfactoren enthalten kann, als solche, welche in jeder der gegebenen Zahlen enthalten sind, und dass er keinen Primfactor öfter enthalten kann, als irgend eine der gegebenen Zahlen.

Aehnlich gestaltet sich die Lösung der anderen Aufgabe, das kleinste gemeinschaftliche Multiplum einer Reihe von gegebenen Zahlen zu bilden (§. 7). Jetzt betrachte man *jede* Primzahl, die in irgend einer der gegebenen Zahlen als Factor enthalten ist, und sehe nach, in welcher sie am häufigsten vorkommt; ebenso oft

nehme man sie als Factor in das kleinste gemeinschaftliche Multiplum auf; sind aber $a, b, c \ldots$ die sämmtlichen Primzahlen, welche in den einzelnen Zerlegungen der gegebenen Zahlen vorkommen, so erhält man nach dieser Regel das gesuchte kleinste gemeinschaftliche Multiplum in der Form

$$a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots,$$

wo z. B. der Exponent α' dadurch bestimmt ist, dass die Primzahl a in mindestens einer der gegebenen Zahlen genau α' mal, in allen übrigen aber nicht öfter als Factor enthalten ist. Der Beweis liegt hier darin, dass die gesuchte Zahl jeden Primfactor enthalten muss, der in einer der gegebenen Zahlen enthalten ist, und zwar mindestens ebenso oft, als diese.

Endlich können wir aus den vorhergehenden Principien noch ein Kriterium ableiten, nach welchem zu erkennen ist, ob eine Zahl

$$m = a^{\alpha} b^{\beta} c^{\gamma} \ldots$$

eine genaue $r$te Potenz einer ganzen Zahl k ist. Dazu ist offenbar erforderlich und hinreichend, dass alle Exponenten $\alpha, \beta, \gamma \ldots$ durch r theilbar sind, wie man sogleich aus der Annahme

$$m = k^r$$

erkennt.

§. 11.

Wir gehen nun zu einer Untersuchung über, welche an sich schon interessant und ausserdem für die Folge von der grössten Wichtigkeit ist. Denken wir uns einmal alle ganzen Zahlen

$$1, 2, 3, 4 \ldots m$$

bis zu einer beliebigen letzten m aufgeschrieben, und zählen wir ab, wie viele von ihnen relative Primzahlen gegen die letzte m sind. Diese Anzahl bezeichnet man in der Zahlentheorie durchgängig mit $\varphi(m)$, wo der Buchstabe φ die Rolle eines Functionszeichens spielt*). Da die Einheit relative Primzahl gegen sich selbst ist, so folgt zunächst

$$\varphi(1) = 1;$$

durch wirkliches Abzählen findet man ferner

*) *Gauss: Disquisitiones Arithmeticae* art. 38.

$$\varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 2,\ \varphi(5) = 4$$

u. s. w. Allein es kommt darauf an, einen allgemeinen Ausdruck für die Function $\varphi(m)$ zu finden, und wir werden sehen, dass man zu diesem Zweck nur die sämmtlichen von einander verschiedenen Primzahlen $a, b, c \dots$ zu kennen braucht, welche in m aufgehen. Unsere Aufgabe ist nämlich identisch mit dieser: die Anzahl der obigen Zahlen zu bestimmen, welche durch keine dieser Primzahlen $a, b, c \dots$ theilbar sind; und diese ist wieder nur ein specieller Fall der folgenden:

Wenn $a, b, c \dots$ relative Primzahlen sind und sämmtlich in einer Zahl m aufgehen, so soll die Anzahl derjenigen der Zahlen

$$1, 2, 3 \dots m \qquad (M)$$

bestimmt werden, welche durch keine der Zahlen $a, b, c \dots$ theilbar sind.

Es zeigt sich nun, wie es häufig geschieht, dass die allgemeinere Aufgabe leichter zu lösen ist, als der direct angegriffene specielle Fall. Zu diesem Zweck scheiden wir zunächst aus dem Zahlencomplex (M) alle diejenigen aus, welche durch die Zahl a theilbar sind; es sind dies offenbar die Zahlen

$$a, 2a, 3a \dots \frac{m}{a}a;$$

die Anzahl derselben ist $m : a$; es bleiben daher, nachdem dieselben aus dem Complex (M) ausgeschieden sind, nur

$$m - \frac{m}{a} = m\left(1 - \frac{1}{a}\right) \qquad (1)$$

Zahlen übrig, welche nicht durch a theilbar sind, und deren Complex wir mit (A) bezeichnen wollen.

Aus diesem Complex (A) sind nun zunächst alle durch b theilbaren Zahlen auszuscheiden; es sind dies offenbar alle diejenigen Zahlen des Complexes (M), welche der doppelten Forderung genügen, erstens dass sie nicht durch a, zweitens dass sie durch b theilbar sind. Alle Zahlen nun, welche der zweiten Forderung genügen, sind die folgenden

$$b, 2b, 3b, \dots \frac{m}{b}b;$$

damit aber eine dieser Zahlen, z. B. rb, auch der ersten Forderung genüge, ist erforderlich und hinreichend, dass der Coefficient r

nicht durch a theilbar sei; denn da der Annahme nach a und b relative Primzahlen sind, so ist rb theilbar oder nicht theilbar durch a, je nachdem r durch a theilbar ist oder nicht (§. 5, 2.). Die Anzahl der noch aus dem Complex (A) auszuscheidenden Zahlen stimmt daher überein mit der Anzahl derjenigen der Zahlen

$$1, 2, 3 \ldots \frac{m}{b},$$

welche nicht durch a theilbar sind. Da nun m durch a und b, folglich auch durch ab theilbar ist, so ist die letzte dieser Zahlen $m : b$ theilbar durch a; unsere Frage ist also dieselbe für die Zahl $m : b$ wie diejenige, welche wir durch den ersten Schritt für die Zahl m gelöst und durch die Formel (1) beantwortet haben. Die Anzahl der aus (A) auszuscheidenden Zahlen ist daher gleich

$$\frac{m}{b}\left(1-\frac{1}{a}\right)$$

und wir erhalten

$$m\left(1-\frac{1}{a}\right)-\frac{m}{b}\left(1-\frac{1}{a}\right)=m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right) \qquad (2)$$

als Anzahl derjenigen im Complex (A) enthaltenen Zahlen, welche nicht durch b theilbar sind, oder, was dasselbe ist, als Anzahl derjenigen in (M) enthaltenen Zahlen, welche weder durch a noch durch b theilbar sind.

Bezeichnen wir den Complex dieser Zahlen mit (B), so kann man in derselben Weise fortfahren und gelangt so durch Induction zu dem Resultat, dass die Anzahl derjenigen in (M) enthaltenen Zahlen (K), welche durch keine der Zahlen $a, b, c \ldots k$ theilbar sind, gleich

$$m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\cdots\left(1-\frac{1}{k}\right) \qquad (3)$$

ist. Um die Allgemeingültigkeit dieses Gesetzes nachzuweisen, nehmen wir an, dass die Richtigkeit desselben für die Zahlen $a, b, c \ldots k$ schon bewiesen sei, und untersuchen, was geschieht, wenn zu denselben noch eine andere l hinzukommt, wobei natürlich wieder vorausgesetzt wird, erstens dass l in m aufgeht, zweitens dass l relative Primzahl gegen jede der vorhergehenden Zahlen $a, b, c \ldots k$ ist.

Um die Anzahl aller in (M) enthaltenen Zahlen zu bestimmen, welche durch keine der Zahlen $a, b, c \ldots k, l$ theilbar sind, haben

wir aus dem Complex (K) derjenigen Zahlen, welche durch keine der Zahlen $a, b, c \ldots k$ theilbar sind, und deren Anzahl durch die Formel (3) gegeben ist, nur noch die auszuscheiden, welche durch l theilbar sind; es sind dies alle diejenigen in (M) enthaltenen Zahlen, welche erstens nicht theilbar durch $a, b, c \ldots k$, zweitens theilbar durch l sind. Alle durch l theilbaren Zahlen des Complexes (M) sind diese

$$l, 2l, 3l \ldots \frac{m}{l} l,$$

und damit irgend eine derselben, z. B. rl, durch keine der Zahlen $a, b \ldots k$ theilbar sei, ist erforderlich und hinreichend, dass der Coefficient r dieselbe Eigenschaft habe. Die Anzahl der auszuscheidenden Zahlen stimmt daher überein mit der Anzahl derjenigen unter den Zahlen

$$1, 2, \ldots \frac{m}{l},$$

welche durch keine der Zahlen $a, b \ldots k$ theilbar sind; diese ist aber nach der als richtig vorausgesetzten Formel (3) gleich

$$\frac{m}{l}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right);$$

nach Ausscheidung derselben aus dem Complex (K) bleiben daher

$$m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right)$$
$$-\frac{m}{l}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right)$$
$$=m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right)\left(1-\frac{1}{l}\right)$$

Zahlen übrig, nämlich diejenigen, welche durch keine der Zahlen $a, b, c \ldots k, l$ theilbar sind.

Hiermit ist die Allgemeingültigkeit unseres Satzes bewiesen; kehren wir nun zu unserer ursprünglichen Aufgabe zurück, so erhalten wir das Resultat*):

---

*) *Euler*: *Theoremata arithmetica nova methodo demonstrata*, Comm. nov. Ac. Petrop. VIII. p. 74. *Speculationes circa quasdam insignes proprietates numerorum*, Acta Petrop. IV, 2. p. 18. — Eine höchst werthvolle Sammlung der arithmetischen Abhandlungen *Euler's* ist von den Brüdern *Fuss* unter folgendem Titel herausgegeben: *Leonhardi Euleri Commentationes Arithmeticae Collectae*. Petropoli 1849. 2 tom.

Sind a, b . . . k, l die sämmtlichen von einander verschiedenen in m aufgehenden Primzahlen, so ist

$$\varphi(m) = m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right)\left(1-\frac{1}{l}\right)$$

die Anzahl aller derjenigen der Zahlen

$$1, 2 \ldots m,$$

welche relative Primzahlen gegen die letzte m sind.

Denn damit irgend eine Zahl relative Primzahl gegen m sei, ist erforderlich und hinreichend, dass sie durch keine der in m aufgehenden absoluten Primzahlen theilbar sei.

Wir können dem gefundenen Ausdruck eine andere Form geben, indem wir m als Product von Primzahl-Potenzen darstellen; da $a, b, c \ldots$ die sämmtlichen von einander verschiedenen in m aufgehenden Primzahlen sind, so hat m die Form

$$m = a^\alpha b^\beta c^\gamma \ldots,$$

und es wird

$$\varphi(m) = (a-1)\, a^{\alpha-1} \,.\, (b-1)\, b^{\beta-1} \,.\, (c-1)\, c^{\gamma-1} \ldots$$

Um unsern Satz an einem Beispiel zu prüfen, wählen wir $m = 60$; die sämmtlichen Zahlen, welche nicht grösser als 60 und relative Primzahlen gegen 60 sind, bilden die Reihe

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59,

und ihre Anzahl ist $= 16$; in der That finden wir nach der obigen Formel, da 2, 3, 5 sämmtliche in 60 aufgehende Primzahlen sind,

$$\varphi(60) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16.$$

§. 12.

Aus der gefundenen Form der Function $\varphi(m)$ geht auch noch folgender Satz hervor: *Sind m und m′ zwei relative Primzahlen, so ist*

$$\varphi(mm') = \varphi(m)\, \varphi(m').$$

Denn sind $a, b, c \ldots$ sämmtliche in m, und $a', b', c' \ldots$ sämmtliche in m' aufgehende Primzahlen, so stimmt, da m und m' relative Primzahlen sind, keine Primzahl der einen Reihe mit einer der andern überein, d. h. alle Primzahlen

$$a, b, c \ldots a', b', c' \ldots$$

sind von einander verschieden. Sie gehen ferner sämmtlich in dem Product mm' auf, und umgekehrt muss jede in mm' aufgehende Primzahl, da sie in einem der beiden Factoren m, m' aufgehen muss, mit einer dieser Primzahlen übereinstimmen. Also sind dies die sämmtlichen von einander verschiedenen in mm' aufgehenden Primzahlen; hieraus folgt

$$\varphi(mm)' = mm' \left\{ \begin{array}{l} \left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{e}\right)\cdots \\ \left(1-\frac{1}{a'}\right)\left(1-\frac{1}{b'}\right)\left(1-\frac{1}{c'}\right)\cdots \end{array} \right\}$$

Da nun andererseits

$$\varphi(m) = m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\cdots$$

und

$$\varphi(m') = m'\left(1-\frac{1}{a'}\right)\left(1-\frac{1}{b'}\right)\left(1-\frac{1}{c'}\right)\cdots$$

ist, so ergiebt sich durch den unmittelbaren Anblick die Richtigkeit des zu beweisenden Satzes.

So ist z. B.

$$\varphi(60) = \varphi(4 \,.\, 15) = \varphi(4)\,\varphi(15) = 2 \,.\, 8 = 16.$$

Uebrigens leuchtet ein, dass der soeben bewiesene Satz ohne Weiteres auf ein Product aus beliebig vielen Zahlen $m, m', m'' \ldots$ ausgedehnt werden kann, welche sämmtlich unter einander relative Primzahlen sind; denn es ist z. B.

$$\varphi(mm'm'') = \varphi(m)\,\varphi(m'm'') = \varphi(m)\,\varphi(m')\,\varphi(m'')$$

und ähnlich für eine grössere Anzahl von Factoren.

§. 13.

Die Aufgabe, den Werth der Function $\varphi(m)$ zu bestimmen, ist eigentlich nur ein specieller Fall von der folgenden:

Wenn δ irgend ein Divisor der Zahl $m = n\delta$ ist, so soll die die Anzahl derjenigen der Zahlen

$$1, 2, 3 \ldots m$$

bestimmt werden, welche mit m den grössten gemeinschaftlichen Divisor δ haben.

Wir können dieselbe sogleich auf den frühern speciellen Fall

zurückführen. Zunächst leuchtet nämlich ein, dass die Zahlen, um welche es sich handelt, unter den Vielfachen von δ, also unter den Zahlen

$$\delta,\ 2\delta,\ 3\delta, \ldots n\delta$$

zu suchen sind. Damit nun δ der grösste gemeinschaftliche Divisor von $m = n\delta$ und einer Zahl von der Form $r\delta$ sei, ist erforderlich und hinreichend, dass der Coefficient r relative Primzahl gegen n sei; die gesuchte Anzahl ist daher zugleich die Anzahl derjenigen der Zahlen

$$1, 2, 3 \ldots n,$$

welche relative Primzahlen gegen die letzte n derselben sind; diese Anzahl ist folglich $= \varphi(n)$. Offenbar geht diese allgemeinere Aufgabe wieder in die frühere über, wenn der Divisor $\delta = 1$ ist.

Aus der Lösung dieser Aufgabe lässt sich nun ein schöner Satz über die Function $\varphi(m)$ ableiten, der in späteren Untersuchungen eine grosse Rolle spielt. Schreiben wir einmal alle Divisoren

$$\delta', \delta'', \delta''' \ldots$$

der Zahl

$$m = n'\delta' = n''\delta'' = n'''\delta''' = \ldots$$

auf, und theilen wir alle m Zahlen

$$1, 2, 3 \ldots m$$

in ebenso viele Gruppen ein, als es Divisoren δ von m giebt, indem wir alle die Zahlen, welche mit m den grössten gemeinschaftlichen Divisor δ' haben, und deren Anzahl nach dem Vorhergehenden $= \varphi(n')$ ist, in die erste Gruppe, ebenso alle die $\varphi(n'')$ Zahlen, welche mit m den grössten gemeinschaftlichen Divisor δ'' haben, in die zweite Gruppe aufnehmen u. s. f. So leuchtet ein, dass jede der m Zahlen in eine, aber auch nur in eine solche Gruppe aufgenommen wird, und es muss daher das Aggregat der Zahlen

$$\varphi(n'), \varphi(n''), \varphi(n''') \ldots$$

welche angeben, wie viele Zahlen der ersten, zweiten, dritten u. s. w. Gruppe angehören, mit der Anzahl m der sämmtlichen in diese Gruppen vertheilten Zahlen übereinstimmen. Da nun die Zahlen $n', n'', n''' \ldots$ die sämmtlichen Divisoren der Zahl m bilden, so erhalten wir folgenden Satz*):

---

*) *Gauss: D. A.* art. 39.

Durchläuft n alle Divisoren einer Zahl m, so ist die entsprechende Summe

$$\Sigma \varphi(n) = m.$$

Es wird gut sein, diesen Satz wieder an einem Beispiel zu prüfen. Nehmen wir $m = 60$, so sind die Zahlen

1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

die sämmtlichen Divisoren n von 60. Nun ist

$$\begin{array}{llll} \varphi(1) = 1, & \varphi(2) = 1, & \varphi(3) = 2, & \varphi(4) = 2, \\ \varphi(5) = 4, & \varphi(6) = 2, & \varphi(10) = 4, & \varphi(12) = 4, \\ \varphi(15) = 8, & \varphi(20) = 8, & \varphi(30) = 8, & \varphi(60) = 16; \end{array}$$

uud die Summe aller dieser Zahlen ist in der That $= 60$.

§. 14.

Der soeben gegebene Beweis dieses wichtigen Satzes über die Function $\varphi(m)$ ergab sich unmittelbar aus dem Begriff dieser Function ohne Hülfe der vorher für dieselbe gefundenen Form und ohne alle Rechnung*); es wird aber gut sein, noch einen zweiten Beweis hinzuzufügen, welcher mehr rechnend zu Werke geht und die früher abgeleitete Form der Function und die daraus gezogenen Folgerungen voraussetzt.

Jeder Divisor n der Zahl

$$m = a^{\alpha} b^{\beta} c^{\gamma} \ldots$$

hat die Form

$$n = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$$

wo wie früher $a, b, c \ldots$ von einander verschiedene Primzahlen bedeuten. Da also $a^{\alpha'}, b^{\beta'}, c^{\gamma'} \ldots$ unter einander relative Primzahlen sind, so ist

$$\varphi(n) = \varphi(a^{\alpha'})\, \varphi(b^{\beta'})\, \varphi(c^{\gamma'}) \ldots$$

Um nun alle Divisoren n der Zahl m zu erhalten, muss man

*) Dieser Satz charakterisirt umgekehrt die Function $\varphi(m)$ vollständig, so dass aus ihm auch die (in §. 11 gefundene) Form derselben abgeleitet werden kann; siehe die Supplemente VII, §. 138.

$$\begin{array}{lll} \alpha' & \text{die Zahlen} & 0, 1, 2 \ldots \alpha \\ \beta' & \text{"} \quad \text{"} & 0, 1, 2 \ldots \beta \\ \gamma' & \text{"} \quad \text{"} & 0, 1, 2 \ldots \gamma \end{array}$$

u. s. w.

durchlaufen lassen. Bildet man nun das Aggregat aller entsprechenden Werthe $\varphi(n)$, so leuchtet ein, dass dasselbe mit dem Product aus den folgenden Summen

$$\begin{array}{l} \varphi(1) + \varphi(a) + \varphi(a^2) + \cdots + \varphi(a^\alpha) \\ \varphi(1) + \varphi(b) + \varphi(b^2) + \cdots + \varphi(b^\beta) \\ \varphi(1) + \varphi(c) + \varphi(c^2) + \cdots + \varphi(c^\gamma) \end{array}$$

u. s. w.

übereinstimmt. Die erste dieser Summen ist aber gleich

$$\begin{aligned} 1 + (a-1) + (a-1)\, a + \cdots + (a-1)\, a^{\alpha-1} \\ = 1 + (a^\alpha - 1) = a^\alpha; \end{aligned}$$

ebenso ist b^β die zweite, c^γ die dritte Summe u. s. f. Es ergiebt sich daher, dass das Aggregat

$$\Sigma\, \varphi(n) = a^\alpha \,.\, b^\beta \,.\, c^\gamma \ldots = m$$

ist, was zu beweisen war.

§. 15.

Wir wenden uns nun noch zu einer Aufgabe, deren Lösung zu einem rein arithmetischen Beweise eines Satzes führt, welcher sonst gewöhnlich durch andere Betrachtungen erwiesen wird. Es handelt sich darum, wenn m eine beliebige ganze Zahl und p eine beliebige Primzahl ist, den Exponenten der höchsten Potenz von p zu bestimmen, welche in der Facultät

$$m! = 1 \,.\, 2 \,.\, 3 \ldots m$$

aufgeht. Bezeichnen wir mit m' die grösste in dem Bruch $m : p$ enthaltene ganze Zahl, so sind unter den m Factoren von $m!$ nur die folgenden m' durch p theilbar

$$p, 2p, 3p \ldots m'p;$$

und da die übrigen Factoren bei unserer Frage keine Rolle spielen, so stimmt der gesuchte Exponent mit dem Exponenten der höchsten Potenz von p überein, welche in dem Product

$$1 \,.\, 2 \ldots m' \,.\, p^{m'}$$

dieser Multipla von p aufgeht, und ist daher gleich der Summe aus m' und dem Exponenten der höchsten Potenz von p, welche in der Facultät

$$m'! = 1 \,.\, 2 \ldots m'$$

aufgeht. Hieraus ergiebt sich unmittelbar, dass der gesuchte Exponent gleich

$$m' + m'' + m''' + \cdots$$

ist, wo m'', m''' ... die grössten in den Brüchen $m' : p$, $m'' : p$ ... enthaltenen ganzen Zahlen bedeuten. Offenbar ist die Reihe der Zahlen m', m'', m''' ... eine abnehmende und folglich eine endliche; der gesuchte Exponent wird $= 0$ sein, wenn $p > m$ ist; denn dann ist schon $m' = 0$. Es mag beiläufig noch bemerkt werden, dass die Zahlen m', m'', m''' ... auch die grössten resp. in den Brüchen $m : p$, $m : p^2$, $m : p^3$ ... enthaltenen ganzen Zahlen sind; ist nämlich r die grösste in $m : a$, und s die grösste in $r : b$ enthaltene ganze Zahl, so ist s auch stets die grösste in $m : ab$ enthaltene ganze Zahl.

Ist z. B. $m = 60$ und $p = 7$, so ist die grösste in

$$\frac{60}{7} \text{ enthaltene ganze Zahl } m' = 8$$

und die grösste in

$$\frac{8}{7} \text{ oder in } \frac{60}{49} \text{ enthaltene ganze Zahl } m'' = 1$$

und die grösste in

$$\frac{1}{7} \text{ oder in } \frac{60}{243} \text{ enthaltene ganze Zahl } m''' = 0;$$

also ist

$$7^{8+1} = 7^9$$

die höchste Potenz von 7, welche in der Facultät $60!$ aufgeht.

Durch das so gewonnene Resultat sind wir in den Stand gesetzt, folgenden Satz zu beweisen: *Ist*

$$m = f + g + h + \cdots,$$

so ist

$$\frac{m!}{f!\, g!\, h! \ldots}$$

eine ganze Zahl.

Denn wenn p irgend eine im Nenner aufgehende Primzahl ist, und wenn wir eine der frühern analoge Bezeichnung beibehalten, so sind

$$f' + f'' + f''' + \cdots$$
$$g' + g'' + g''' + \cdots$$
$$h' + h'' + h''' + \cdots$$
u. s. w.

die Exponenten der höchsten Potenzen von p, welche resp. in $f!$, in $g!$, in $h!$ u. s. w. aufgehen, und folglich ist

$$(f' + g' + h' + \cdots) + (f'' + g'' + h'' + \cdots) + (f''' + g''' + h''' + \cdots) + \cdots$$

der Exponent der höchsten Potenz von p, welche in dem ganzen Nenner aufgeht. Andererseits ist

$$m' + m'' + m''' + \cdots$$

der Exponent der höchsten im Zähler aufgehenden Potenz von p; es ist daher nur zu zeigen, dass die letztere Summe nicht kleiner ist als die erstere. Da nun

$$\frac{m}{p} = \frac{f}{p} + \frac{g}{p} + \frac{h}{p} + \cdots$$

ist, so leuchtet unmittelbar ein, dass

$$m' \geqq f' + g' + h' + \cdots$$

sein muss; hieraus folgt aber wieder

$$\frac{m'}{p} \geqq \frac{f'}{p} + \frac{g'}{p} + \frac{h'}{p} + \cdots$$

also *a fortiori*

$$m'' \geqq f'' + g'' + h'' + \cdots$$

u. s. f., woraus die Richtigkeit der obigen Behauptung erhellt. Da nun jede im Nenner aufgehende Primzahl mindestens ebenso oft im Zähler aufgeht, so ist der Zähler theilbar durch den Nenner, der Bruch selbst also wirklich eine ganze Zahl.

Hieraus folgt auch, dass jedes Product von m successiven ganzen Zahlen

$$(a+1)\,(a+2)\,\ldots\,(a+m-1)\,(a+m)$$

stets durch das Product der ersten m ganzen Zahlen

$$m! = 1\,.\,2\,.\,3\,\ldots\,(m-1)\,m$$

theilbar ist; denn der Quotient

$$\frac{(a+1)\,(a+2)\,\ldots\,(a+m-1)\,(a+m)}{1\quad.\quad2\quad\ldots\quad(m-1)\quad m}$$

ist gleich

$$\frac{(a+m)!}{a!\;m!}$$

und folglich eine ganze Zahl.

§. 16.

Hiermit beschliessen wir die Reihe der Sätze über die Theilbarkeit der Zahlen; aber es ist wohl der Mühe werth, an dieser Stelle noch einen Rückblick auf den Entwicklungsgang dieser unserer bisherigen Untersuchungen zu werfen. Da beobachten wir nun vor allen Dingen, dass das ganze Gebäude auf *einem* Fundament ruht, nämlich auf dem Algorithmus, welcher dazu dient, den grössten gemeinschaftlichen Theiler zweier Zahlen aufzufinden. Dass alle nachfolgenden Sätze, wenn sie sich auch zum Theil auf erst später eingeführte Begriffe, wie die der relativen und absoluten Primzahlen, beziehen, doch nur einfache Consequenzen aus dem Resultat jener ersten Untersuchung sind, ist so evident, dass man unmittelbar zu der Behauptung berechtigt wird: in jeder analogen Theorie, in welcher ein dem Algorithmus des grössten gemeinschaftlichen Divisors ähnlicher Algorithmus existirt, muss auch ein System von Folgerungen Statt finden, welches dem in unserer Theorie entwickelten ganz analog ist. In der That giebt es solche Theorieen; betrachtet man z. B. alle in der Form

$$t + u\sqrt{-a}$$

enthaltenen Zahlen, in welcher a eine bestimmte positive, t und u dagegen unbestimmte reelle ganze Zahlen bedeuten, und nennt dieselben ganze complexe Zahlen oder kurz ganze Zahlen, so kann man den Begriff des Vielfachen so fassen, dass eine solche Zahl ein Vielfaches von einer zweiten heisst, wenn die erste ein Product aus der zweiten und irgend einer dritten solchen Zahl ist. Aber nur für gewisse besondere Werthe von a, z. B. für $a = 1$, lässt sich die Frage nach den gemeinschaftlichen Divisoren zweier Zahlen durch einen endlich abschliessenden Algorithmus beantworten, der dem in unserer reellen Theorie ganz ähnlich ist; es findet daher in der Theorie der Zahlen von der Form $t + u\sqrt{-1}$ auch durchgängige Analogie mit unserer Theorie der reellen Zahlen Statt. Ganz anders verhält es sich, wenn z. B. $a = 11$ ist; in der Theorie der Zahlen von der Form $t + u\sqrt{-11}$ findet unter andern der Satz nicht mehr Statt, dass eine Zahl nur auf eine einzige Weise als Product von nicht weiter zerlegbaren Zahlen dargestellt werden kann; so z. B. lässt sich die Zahl 15 einmal als $3 \cdot 5$, ein

anderes Mal als $(2+\sqrt{-11})\,(2-\sqrt{-11})$ darstellen, obgleich jede der vier Zahlen

$$3,\ 5,\ 2+\sqrt{-11},\ 2-\sqrt{-11}$$

nicht weiter in Factoren von der Form $t+u\sqrt{-11}$ zerlegbar ist. Der Grund dieser interessanten Erscheinung liegt allein darin, dass es bei den Zahlen dieser Form nicht mehr gelingt, einen nach einer endlichen Anzahl von Operationen abschliessenden Algorithmus zur Auffindung der gemeinschaftlichen Divisoren zweier Zahlen zu bilden*).

*) Die Einführung der ganzen complexen Zahlen von der Form $t+u\sqrt{-1}$ rührt von *Gauss* her; eine kurze Darstellung der Elemente dieser neuen Zahlentheorie findet man in seiner Abhandlung *Theoria residuorum biquadraticorum* II, oder in einer Abhandlung von *Dirichlet: Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes* (Crelle's Journal XXIV). Das oben erwähnte abweichende Verhalten anderer Zahlformen hat *Kummer* zur Einführung der *idealen* Zahlen veranlasst (Crelle's Journal XXXV).

Zweiter Abschnitt.

Von der Congruenz der Zahlen.

§. 17.

Bedeutet k irgend eine positive ganze Zahl, so lässt sich jede beliebige ganze Zahl a stets und nur auf eine einzige Weise in die Form

$$a = sk + r$$

bringen, in welcher s eine ganze Zahl und r eine der k Zahlen

$$0, 1, 2 \ldots (k-1)$$

bedeutet. Denn lässt man zunächst s alle ganzen Zahlwerthe von $-\infty$ bis $+\infty$ durchlaufen, so bilden die Zahlen sk die sämmtlichen Multipla von k, und von einem solchen Multiplum sk bis zum nächst grössern $(s+1)k$ excl. giebt es immer nur k Zahlen, nämlich

$$sk, sk+1, sk+2 \ldots sk+(k-1);$$

giebt man daher dem s alle denkbaren ganzen Zahlwerthe, und dem r jedesmal alle jene bestimmten k Werthe, so durchläuft der Ausdruck $sk+r$ wirklich alle ganzen Zahlwerthe a; dass ferner jede Zahl a auf diese Weise nur ein einziges Mal erzeugt wird, leuchtet auf folgende Weise ein. Wenn

$$s'k + r' = sk + r$$

ist, so folgt daraus

$$r' - r = (s - s')k;$$

wenn nun r' ebenfalls eine der k Zahlen $0, 1, 2 \ldots (k-1)$ ist, so ist der absolute Werth von $r'-r$ ebenfalls eine dieser Zahlen, also kleiner als k; da aber $r'-r$ ein Multiplum von k ist, so kann $r'-r$ nur $=0$ sein, woraus $r'=r$ und $s'=s$ folgt.

Wir werden nun im Folgenden sagen, dass die Zahl r der *Rest* der Zahl a in Bezug auf den *Modulus* k ist; sobald ferner zwei Zahlen a und b in Bezug auf denselben Modulus k denselben Rest r lassen, sollen sie *gleichrestig* oder (nach *Gauss*) *congruent* in Bezug auf den Modulus k heissen; da in diesem Fall $a=sk+r$ und $b=s'k+r$ ist, so folgt, dass die Differenz $a-b=(s-s')k$ durch den Modulus k theilbar ist; und umgekehrt, ist $a-b$ durch k theilbar, so sind die Zahlen a und b auch congruent in Bezug auf den Modul k; denn ist r der Rest von a, r' der von b, also

$$a = sk+r, \quad b = s'k+r',$$

so ist

$$a-b = (s-s')k + (r-r');$$

da nun der Voraussetzung nach $a-b$ ein Multiplum von k ist, so muss auch $r'-r$ ein solches sein, was, wie wir vorher gesehen haben, nicht anders möglich ist, als wenn $r'=r$ ist. Man könnte daher congruente Zahlen auch als solche definiren, deren Differenz durch den Modul theilbar ist. (Aus diesem Grunde hat man die Bedeutung des Wortes Rest in der Weise erweitert, dass jede von zwei einander nach dem Modul k congruenten Zahlen a und b ein *Rest* der andern heisst.)

Da man sehr häufig die Congruenz zweier Zahlen a und b in Bezug auf eine dritte k als Modul auszudrücken hat, so ist von *Gauss* *) für dieselbe folgende Bezeichnung eingeführt:

$$a \equiv b \pmod{k}.$$

So ist z. B.

$$3 \equiv -25 \pmod{4}, \quad 65 \equiv 16 \pmod{7}.$$

Da die beiden Zahlen a und b in dem Begriffe der Congruenz dieselbe Rolle spielen, so darf man offenbar die zur Linken und Rechten des Zeichens $\equiv$ stehenden Zahlen mit einander vertauschen. Ferner leuchten aus dem Begriffe der Congruenz leicht die folgenden Sätze ein:

1. Sind a und k zwei beliebige Zahlen, so ist stets

$$a \equiv a \pmod{k}.$$

---

*) *D. A.* art. 2.

2. Ist in Bezug auf denselben Modulus k eine erste Zahl a einer zweiten b, diese wieder einer dritten c congruent, so ist auch die erste a der dritten c in Bezug auf k congruent; in Zeichen: ist

$$a \equiv b \pmod{k}, \quad b \equiv c \pmod{k},$$

so ist auch

$$a \equiv c \pmod{k}.$$

Denn die Reste der drei Zahlen a, b, c sind einander gleich; oder auch, da $a - b$ und $b - c$ Multipla von k sind, so ist auch $(a - b) + (b - c) = a - c$ Multiplum von k.

3. Ist

$$a \equiv b \pmod{k} \text{ und } m \equiv n \pmod{k},$$

so ist auch

$$a + m \equiv b + n \pmod{k} \text{ und } a - m \equiv b - n \pmod{k}.$$

Denn da $a - b$ und $m - n$ Multipla von k sind, so sind auch $(a - b) + (m - n) = (a + m) - (b + n)$ und $(a - b) - (m - n) = (a - m) - (b - n)$ Multipla von k.

Dies lässt sich für eine beliebige Anzahl von Congruenzen erweitern, die sich auf denselben Modulus beziehen; man kann sie addiren und subtrahiren wie Gleichungen.

4. Ist wieder

$$a \equiv b \pmod{k} \text{ und } m \equiv n \pmod{k},$$

so ist auch

$$am \equiv bn \pmod{k}.$$

Denn da $a - b$ ein Vielfaches von k ist, so ist zunächst auch $(a - b)\, m = am - bm$ ein solches, also

$$am \equiv bm \pmod{k};$$

da ferner $m - n$ ein Vielfaches von k ist, so ist auch $b(m - n) = bm - bn$ ein solches, also

$$bm \equiv bn \pmod{k};$$

die beiden Zahlen am und bn sind daher derselben Zahl bm congruent, folglich sind sie auch unter einander congruent.

Auch dieser Satz lässt sich dahin verallgemeinern, dass man eine ganze Reihe von Congruenzen, die sich auf denselben Modul beziehen, mit einander multipliciren kann wie Gleichungen; und hieraus folgt wieder, dass gleich hohe Potenzen zweier congruenten Zahlen wieder congruent sind in Bezug auf denselben Modulus.

5. Die bisherigen Sätze kann man folgendermaassen zusammenfassen. Ist $f(x, y, z \ldots)$ eine ganze rationale Function der

Unbestimmten $x, y, z \ldots$, deren Coefficienten ganze Zahlen sind, und ist in Bezug auf einen und denselben Modulus k

$$a \equiv a',\ b \equiv b',\ c \equiv c' \ldots,$$

so ist auch

$$f(a, b, c \ldots) \equiv f(a', b', c' \ldots) \pmod{k}.$$

6. Etwas anders verhält es sich bei der Division. Ist nämlich

$$am \equiv bm \pmod{k},$$

so kann man hieraus im Allgemeinen nicht mit Sicherheit schliessen, dass auch $a \equiv b \pmod{k}$ sein muss; bezeichnen wir mit δ den grössten gemeinschaftlichen Divisor der beiden Zahlen $m = m'\delta$ und $k = k'\delta$, so folgt aus der obigen Congruenz nur, dass

$$a \equiv b \left(\mathrm{mod.}\, \frac{k}{\delta}\right)$$

sein muss. Denn da $m(a-b)$ durch k, also $m'(a-b)$ durch k' theilbar, und m' relative Primzahl gegen k' ist, so muss $(a-b)$ durch k' theilbar sein.

7. Ist

$$a \equiv b \pmod{k}$$

und m irgend ein Divisor von k, so ist auch

$$a \equiv b \pmod{m}.$$

Denn $a-b$ ist ein Multiplum von k, und k ein Multiplum von m; also ist $a-b$ auch ein Multiplum von m.

8. Ist

$a \equiv b \pmod{k}$ und $a \equiv b \pmod{l}$ und $a \equiv b \pmod{m}$ u. s. w., so ist auch

$$a \equiv b \pmod{h},$$

wo h das kleinste gemeinschaftliche Multiplum von $k, l, m \ldots$ bezeichnet. Denn $a-b$ ist ein gemeinschaftliches Multiplum aller dieser Zahlen, also auch Multiplum von h.

Hieraus folgt auch noch als ein besonders bemerkenswerther specieller Fall, dass, wenn eine Congruenz richtig ist in Bezug auf eine Reihe von Moduln, die sämmlich unter einander relative Primzahlen sind, dieselbe auch in Bezug auf einen Modul gilt, welcher das Product aus allen jenen Moduln ist.

Wir bemerken schliesslich, dass auch *negative* Moduln k zugelassen werden; das Zeichen $a \equiv b \pmod{k}$ bedeutet auch dann,

dass die Differenz $a-b$ durch k theilbar ist; offenbar behalten die vorstehenden Sätze auch nach dieser Erweiterung ihre volle Gültigkeit.

§. 18.

Da jede beliebige Zahl a ihrem Reste r in Bezug auf den (positiven) Modul k congruent ist, so ist jede Zahl a einer der k Zahlen

$$0, 1, 2 \ldots (k-1)$$

congruent; sie kann aber auch nur einer dieser Zahlen congruent sein, denn sonst müssten ja auch unter diesen k Resten mindestens zwei einander congruent sein, was offenbar nicht der Fall ist. Theilen wir daher sämmtliche Zahlen in *Classen* ein nach dem Princip, dass wir jedesmal zwei Zahlen in dieselbe oder in verschiedene Classen werfen, je nachdem sie in Bezug auf den Modulus k congruent sind oder nicht, so ist die *Anzahl* dieser Classen offenbar $= k$; die eine enthält sämmtliche Zahlen, welche $\equiv 0 \pmod{k}$, d. h. durch k theilbar sind; die folgende Classe enthält alle Zahlen, welche $\equiv 1 \pmod{k}$ sind, u. s. f.

Greift man nun aus jeder dieser Classen nach Belieben ein Individuum heraus, so hat das so gebildete System von k Zahlen die charakteristische Eigenschaft, dass jede beliebige ganze Zahl stets einer und auch nur einer von diesen k Zahlen congruent ist; ein solches System, wie es z. B. auch die Zahlen

$$0, 1, 2 \ldots (k-1)$$

bilden, nennt man ein *vollständiges System nicht congruenter* (oder *incongruenter*) *Zahlen* oder ein *vollständiges Restsystem* in Bezug auf den Modul k; offenbar bilden auch die Zahlen

$$1, 2, 3 \ldots k$$

und ebenso je k successive ganze Zahlen ein solches System.

Alle Zahlen, welche einer und derselben Classe angehören, haben nun mehrere allen gemeinschaftliche Eigenschaften, so dass sie in Bezug auf den Modul fast die Rolle einer einzigen Zahl spielen. Wir haben schon früher gesehen, dass jede Zahl, welche in einer Congruenz als Summand oder als Factor auftritt, unbeschadet der Richtigkeit der Congruenz durch jede andere ihr congruente, d. h. derselben Classe angehörige Zahl ersetzt werden

darf. Ein anderes Element, welches allen in einer Classe enthaltenen Individuen gemeinschaftlich ist, bildet der grösste Divisor, den sie mit dem Modul k gemeinschaftlich haben; denn sind a und b zwei congruente Zahlen, so ist

$$a = b + sk,$$

und folglich ist jeder gemeinschaftliche Divisor von a und k auch gemeinschaftlicher Divisor von b und k. Man kann daher nach diesem grössten gemeinschaftlichen Divisor die Classen wieder in Gruppen eintheilen, und da die Zahlen

$$1, 2 \ldots k$$

ein vollständiges System incongruenter Zahlen bilden, so ist (nach §. 13), wenn δ irgend einen Divisor von $k = n\delta$ bezeichnet, $\varphi(n)$ die Anzahl derjenigen Classen, welche solche Zahlen enthalten, die δ zum grössten gemeinschaftlichen Divisor mit dem Modul k haben. Speciell ist also $\varphi(k)$ die Anzahl derjenigen Classen, welche nur Zahlen enthalten, die relative Primzahlen gegen den Modulus k sind.

Von besonderer Wichtigkeit für spätere Untersuchungen ist auch noch folgender Satz:

Ist a relative Primzahl gegen den Modulus k, und setzt man in dem linearen Ausdruck $ax + b$ für x der Reihe nach alle k Glieder eines vollständigen Systems incongruenter Zahlen ein, so bilden die so entstehenden Werthe dieses Ausdrucks wieder ein vollständiges System incongruenter Zahlen.

Da nämlich aus

$$ax + b \equiv ay + b \pmod{k}$$

auch

$$ax \equiv ay \pmod{k}$$

und, da a relative Primzahl gegen k ist, nach §. 17, 6. auch

$$x \equiv y \pmod{k}$$

folgt, so ergiebt sich, dass alle Werthe des Ausdrucks $ax + b$, welche incongruenten Werthen von x entsprechen, ebenfalls incongruent sind; setzt man daher für x alle k incongruenten Zahlen ein, so erhält der Ausdruck $ax + b$ auch k incongruente Werthe, welche, da es überhaupt nur k Classen giebt, ein vollständiges System incongruenter Zahlen bilden.

§. 19.

Betrachten wir jetzt den Ausdruck ax, in welchem a wieder relative Primzahl gegen den Modul k ist, und setzen wir wieder für x der Reihe nach die Glieder eines vollständigen Systems incongruenter Zahlen ein, aber nicht alle, sondern nur diejenigen

$$a_1, a_2, a_3 \ldots,$$

welche relative Primzahlen gegen den Modul k sind, und deren Anzahl nach dem vorigen Paragraphen gleich $\varphi(k)$ ist, so leuchtet erstens ein, dass die Werthe des Ausdrucks ax, d. h. die Producte

$$aa_1, \quad aa_2, \quad aa_3 \ldots$$

sämmtlich incongruent sind, ferner, dass dieselben sämmtlich wieder relative Primzahlen gegen k sind; es wird daher jedes dieser Producte einem und nur einem Gliede der Reihe

$$a_1, a_2, a_3 \ldots$$

congruent sein. Wir können daher setzen

$$\left.\begin{aligned} aa_1 &\equiv b_1 \\ aa_2 &\equiv b_2 \\ aa_3 &\equiv b_3 \end{aligned}\right\} (\text{mod.}\, k),$$

u. s. w.

wo nun die Zahlen

$$b_1, b_2, b_3 \ldots$$

vollständig, wenn auch in anderer Ordnung, mit den Zahlen

$$a_1, a_2, a_3 \ldots$$

übereinstimmen, so dass namentlich

$$a_1 a_2 a_3 \ldots \equiv b_1 b_2 b_3 \ldots$$

sein wird. Bezeichnen wir zur Abkürzung dieses Product mit P, und multipliciren wir die vorstehenden $\varphi(k)$ Congruenzen mit einander, so erhalten wir daher

$$a^{\varphi(k)} \,.\, P \equiv P \;(\text{mod.}\, k).$$

Nun ist aber P ein Product von lauter Zahlen, die relative Primzahlen gegen den Modul sind, also selbst relative Primzahl gegen den Modul k; es ist daher nach §. 17, 6. gestattet, die vorstehende Congruenz durch den gemeinschaftlichen Factor P beider Seiten ohne Weiteres zu dividiren. Auf diese Weise erhalten wir die Congruenz

$$a^{\varphi(k)} \equiv 1 \text{ (mod. } k);$$

in Worten kann man diesen höchst wichtigen Satz folgendermaassen aussprechen:

Ist a relative Primzahl gegen die positive Zahl k, und erhebt man a zu einer Potenz, deren Exponent $\varphi(k)$ angiebt, wie viele der Zahlen

$$1, 2, 3 \ldots k$$

relative Primzahlen gegen k sind, so lässt diese Potenz, durch k dividirt, stets den Rest 1.

Nehmen wir z. B. $k = 15$, $a = 2$, so ist a wirklich relative Primzahl gegen k; nun ist $\varphi(k) = \varphi(15) = \varphi(3)\,\varphi(5) = 8$; es muss daher 2^8, durch 15 dividirt, den Rest 1 lassen; in der That ist

$$2^8 = 256 = 17 \,.\, 15 + 1.$$

Es kann übrigens vorkommen, dass auch Potenzen von a mit niedrigerm Exponenten als $\varphi(k)$ denselben Rest 1 geben. Dies tritt wirklich in dem eben gewählten Beispiel ein, denn es ist auch

$$2^4 = 16 = 1 \,.\, 15 + 1.$$

Specialisiren wir unsern Satz für den Fall, dass k nur durch eine einzige Primzahl p theilbar, also

$$k = p^{\pi}, \;\; \varphi(k) = (p-1)p^{\pi-1}$$

ist, so erhalten wir den Satz:

Ist p eine Primzahl und a irgend eine durch p nicht theilbare Zahl, so ist

$$a^{(p-1)p^{\pi-1}} \equiv 1 \text{ (mod. } p^{\pi}).$$

Nehmen wir ferner hierin $\pi = 1$, so erhalten wir einen berühmten Satz, der zuerst von *Fermat* aufgestellt ist und daher der Fermat'sche Satz heisst:

Ist p eine Primzahl und a irgend eine durch p nicht theilbare Zahl; so ist

$$a^{p-1} \equiv 1 \text{ (mod. } p).$$

Man kann diesen Satz so umformen, dass er auch für den Fall gültig bleibt, wenn a durch p theilbar ist; zu diesem Zweck braucht man nur die vorstehende Congruenz mit a zu multipliciren, wodurch sie in die folgende

$$a^p \equiv a \text{ (mod. } p)$$

übergeht. Ist nämlich a theilbar durch p, so sind beide Seiten dieser Congruenz $\equiv 0$ (mod. p), also ist sie auch dann noch richtig. Umgekehrt kann man aus dieser Form des Satzes auch wieder die

frühere ableiten; denn sobald a nicht theilbar durch p, also relative Primzahl gegen p ist, darf man beide Seiten dieser Congruenz auch wieder durch a dividiren, ohne den Modul zu ändern.

Kehren wir zu dem allgemeinen Satz zurück, der zuerst von *Euler* *) bewiesen ist und den Namen des verallgemeinerten Fermat'schen Satzes führt, so können wir denselben auch in folgender Weise aussprechen: Sind $p, r, s \dots$ von einander verschiedene absolute Primzahlen, und ist a durch keine dieser Primzahlen theilbar, so ist stets

$$a^{(p-1)p^{\pi-1} \cdot (r-1)r^{\varrho-1} \cdot (s-1)s^{\sigma-1} \dots} \equiv 1 \pmod{p^\pi r^\varrho s^\sigma \dots},$$

wo $\pi, \varrho, \sigma \dots$ irgend welche ganze positive Zahlen bedeuten.

§. 20.

Es ist wohl nicht überflüssig, dem vorhergehenden Beweise dieses wichtigen Satzes einen zweiten hinzuzufügen, der gradatim zu Werke geht und sich zunächst auf den binomischen Satz stützt. Ist p irgend eine ganze positive Zahl, so ist zufolge dieses Satzes bekanntlich

$$(a+b)^p =$$
$$a^p + \frac{p}{1} a^{p-1} b + \dots + \frac{p!}{r!(p-r)!} a^{p-r} b^r + \dots + b^p;$$

hierin sind (nach §. 15) alle Coefficienten ganze Zahlen. Ist aber p eine Primzahl, so können wir hinzufügen, dass alle Coefficienten mit Ausnahme des ersten und letzten, welche $= 1$ sind, durch p theilbar sind; denn der Zähler des Bruches

$$\frac{p!}{r!(p-r)!},$$

in welchem r eine der Zahlen $1, 2, 3 \dots (p-1)$ bedeutet, enthält den Factor p, der Nenner dagegen nicht; der Bruch ist also von der Form $pm : n$, wo n nicht theilbar durch p, also auch relative Primzahl gegen p ist; da wir aber ferner wissen, dass dieser Bruch eine ganze Zahl, dass also pm durch n theilbar ist, so muss m durch n theilbar sein; der Bruch hat daher die Form ps, wo der zweite Factor s eine ganze Zahl ist; und folglich ist jeder dieser $(p-1)$ Coefficienten $\equiv 0 \pmod{p}$. Sind daher a und b irgend welche ganze Zahlen, so erhalten wir die folgende Congruenz

$$(a+b)^p \equiv a^p + b^p \pmod{p},$$

*) *Theoremata arithm. nova meth. demonstr.*, Comm. nov. Ac. Petrop. VIII. p. 74.

wobei also vorausgesetzt ist, dass p eine Primzahl ist. Offenbar folgt hieraus weiter

$$(a+b+c)^p \equiv (a+b)^p + c^p \equiv a^p + b^p + c^p \pmod{p}$$

und allgemein für eine beliebige Reihe von n ganzen Zahlen a, $b \ldots h$:

$$(a+b+\cdots+h)^p \equiv a^p + b^p + \cdots + h^p \pmod{p}.$$

Setzen wir hierin $a=1$, $b=1 \ldots h=1$, so erhalten wir für jede beliebige positive ganze Zahl n den Satz:

$$n^p \equiv n \pmod{p}.$$

Da ferner für jede ungerade Primzahl $(-1)^p \equiv -1$, und für die einzige gerade Primzahl $p=2$ ebenfalls $(-1)^p = 1 \equiv -1 \pmod{p}$ ist, so erhalten wir durch Multiplication der vorstehenden Congruenz mit der andern

$$(-1)^p \equiv -1 \pmod{p}$$

die neue

$$(-n)^p \equiv -n \pmod{p}.$$

Also ist der Fermat'sche Satz

$$a^p \equiv a \pmod{p}$$

für jede positive und negative Zahl a bewiesen, während er für $a=0$ unmittelbar evident ist. Wenn nun a nicht durch p theilbar ist, was wir von jetzt annehmen wollen, so folgt hieraus, dass

$$a^{p-1} \equiv 1 \pmod{p}, \text{ d. h. } a^{p-1} = 1 + hp$$

ist, wo h eine ganze Zahl bedeutet. Erheben wir diese Gleichung zur $p$ten Potenz und entwickeln die rechte Seite wieder nach dem binomischen Satze, so zeigt sich, dass alle Glieder mit Ausnahme des ersten Multipla von p^2 sind; wir erhalten daher

$$a^{(p-1)p} = 1 + h'p^2 \text{ oder } a^{(p-1)p} \equiv 1 \pmod{p^2},$$

wo wieder h' eine ganze Zahl bedeutet. So kann man fortfahren, indem man jedesmal wieder zur $p$ten Potenz erhebt, und gelangt auf diese Weise zu der Congruenz

$$a^{(p-1)p^{\pi-1}} \equiv 1 \pmod{p^\pi},$$

deren Allgemeingültigkeit sich in derselben Weise durch den Schluss von π auf $\pi+1$ nachweisen lässt.

Sind nun $r, s \ldots$ ebenfalls Primzahlen, welche nicht in a aufgehen, so ist nach demselben Satze

$$a^{(r-1)r^{\varrho-1}} \equiv 1 \pmod{r^\varrho}, \quad a^{(s-1)s^{\sigma-1}} \equiv 1 \pmod{s^\sigma} \ldots$$

Setzen wir ferner zur Abkürzung

$$h = (p-1)p^{\pi-1} \,.\, (r-1)r^{\varrho-1} \,.\, (s-1)s^{\sigma-1} \ldots$$

und berücksichtigen wir, dass aus jeder Congruenz von der Form

$$a^\alpha \equiv 1 \pmod{m}$$

auch die Congruenz

$$a^h \equiv 1 \pmod{m}$$

folgt, sobald h ein Multiplum von α ist, so ergiebt sich, dass die Congruenz

$$a^h \equiv 1$$

für jeden der Moduln p^π, r^ϱ, $s^\sigma \ldots$ und folglich, da dieselben relative Primzahlen sind, auch für den Modul

$$k = p^\pi r^\varrho s^\sigma \ldots$$

gilt. Hiermit ist also von Neuem der verallgemeinerte Fermat'sche Satz erwiesen.

§. 21.

Es kommt häufig vor, dass eine oder beide Seiten einer Congruenz eine oder mehrere unbestimmte Zahlen $x, y \ldots$ enthalten, und es wird dann die Aufgabe gestellt, alle ganzzahligen Werthe von $x, y \ldots$ zu suchen, durch welche die beiden Seiten der Congruenz wirklich einander congruent werden. Je nach der Anzahl der Unbestimmten $x, y \ldots$ heisst dann eine solche Congruenz eine Congruenz mit einer, zwei oder mehreren *Unbekannten*, ähnlich wie dies bei Gleichungen zu geschehen pflegt. Auch hier nennt man dann solche specielle Werthe von $x, y \ldots$, welche die Congruenz zu einer identischen machen, *Wurzeln* der Congruenz, und das Problem der Auflösung einer Congruenz besteht in der Auffindung ihrer sämmtlichen Wurzeln. Wir werden im Folgenden nur solche Congruenzen betrachten, welche eine einzige Unbekannte x enthalten und ausserdem sich auf die Form

$$ax^m + bx^{m-1} + \cdots + gx + h \equiv 0 \pmod{k}$$

bringen lassen, worin m eine positive ganze Zahl und $a, b \ldots g, h$ ebenfalls gegebene ganze Zahlen bedeuten. Jeder Werth von x, der, in die linke Seite eingesetzt, dieselbe durch den Modul k theilbar macht, heisst also eine Wurzel dieser Congruenz. Kennt man irgend eine solche Wurzel x, so sind offenbar nach §. 17, 5. alle ihr nach dem Modul k congruenten Zahlen, d. h. alle Individuen der Classe, welcher diese Zahl x angehört, ebenfalls Wurzeln der-

selben Congruenz; man sieht alle solche einander congruenten Wurzeln daher nur wie eine einzige Wurzel an, und das Problem der vollständigen Auflösung der Congruenz kommt daher darauf zurück, alle unter einander *incongruenten* Wurzeln derselben aufzufinden.

Ferner leuchtet ein, dass jede Wurzel der obigen Congruenz, sobald

$$a \equiv a', \; b \equiv b' \ldots g \equiv g', \; h \equiv h' \pmod{k}$$

ist, auch eine Wurzel der Congruenz

$$a'x^m + b'x^{m-1} + \cdots + g'x + h' \equiv 0 \pmod{k}$$

sein wird, und umgekehrt. Beide Congruenzen sind daher auch nur wie eine und dieselbe anzusehen; denn beide stellen an die Unbekannte x genau dieselbe Forderung. Hieraus erhellt unmittelbar, dass man aus jeder Congruenz von der obigen Form ohne Weiteres alle diejenigen Glieder fortstreichen darf, deren Coefficienten durch den Modul theilbar sind; der Exponent der höchsten Potenz von x, welche nach dieser vorläufigen Ausscheidung zurückbleibt, heisst dann der *Grad* dieser Congruenz; ist z. B. in der obigen Congruenz der erste Coefficient a nicht durch den Modul k theilbar, so heisst dieselbe eine Congruenz $m$ten Grades.

Wenden wir diese Benennungen z. B. auf die Congruenz

$$x^{\varphi(k)} \equiv 1 \pmod{k}$$

an, so müssen wir sagen, dass dieselbe genau ebenso viele (incongruente) Wurzeln besitzt, als ihr Grad $\varphi(k)$ Einheiten enthält; denn erstens genügen alle relativen Primzahlen gegen den Modul der Congruenz, und diese zerfallen in $\varphi(k)$ Classen; und zweitens kann die Congruenz keine andern Wurzeln haben als diese; denn der grösste gemeinschaftliche Divisor δ einer Wurzel x und des Modul k ist auch gemeinschaftlicher Divisor der Zahlen $x^{\varphi(k)}$ und k, folglich auch (§. 18) der Zahlen 1 und k; folglich kann δ nur $= 1$ sein.

§. 22.

Wir wenden uns nun nach den vorhergehenden allgemeinen Erörterungen zu dem einfachsten speciellen Fall, nämlich zu der Congruenz ersten Grades, welcher man offenbar durch Transposition des bekannten Gliedes stets die Form

$$ax \equiv b \pmod{k} \qquad (1)$$

geben kann. Betrachten wir auch hier zunächst nur den speciellen Fall, in welchem der Coefficient a relative Primzahl gegen den Modul k ist, so ergiebt sich unmittelbar, dass diese Congruenz stets eine, aber auch nur eine Wurzel hat. Denn wir haben früher (§. 18) gesehen, dass die Werthe des Ausdrucks ax, welche man erhält, wenn man für x sämmtliche k Individuen eines vollständigen Systems incongruenter Zahlen einsetzt, wieder ein solches System bilden; unter den Werthen dieses Ausdrucks wird sich daher auch einer und nur einer finden, welcher derselben Classe angehört wie b, d. h. welcher $\equiv b$ ist. Der verallgemeinerte Fermat'sche Satz giebt nun auch ein Mittel an die Hand, die Wurzel dieser Congruenz unmittelbar zu bestimmen; offenbar genügt jede Zahl

$$x \equiv b \,.\, a^{\varphi(k)-1} \pmod{k}$$

der obigen Congruenz. So findet man z. B., dass alle Wurzeln der Congruenz

$$2x \equiv -3 \pmod{15}$$

durch die Formel

$$x \equiv -3 \,.\, 2^7 \equiv 6 \pmod{15}$$

gegeben werden.

Wenden wir uns nun dem allgemeinen Fall zu und nehmen wir an, es sei δ der grösste gemeinschaftliche Divisor des Coefficienten a und des Modul k, so leuchtet zunächst ein, dass, wenn die Congruenz überhaupt eine Wurzel x besitzt, auch b durch δ theilbar sein muss; denn da ax mit dem Modul k den gemeinschaftlichen Divisor δ hat, so muss auch $b \equiv ax$ durch δ theilbar sein. Dies ist also eine unerlässliche Bedingung für die Möglichkeit der Congruenz; dass sie auch hinreichend für dieselbe ist, wird sich sogleich zeigen.

Gesetzt nun, es sei x eine Wurzel der Congruenz, also

$$ax = b + mk,$$

wo m irgend eine ganze Zahl, so folgt hieraus, wenn $a = a'\delta$, $b = b'\delta$, $k = k'\delta$ gesetzt wird, $a'x = b' + mk'$, d. h. jede Wurzel der ursprünglichen Congruenz ist auch Wurzel der Congruenz

$$a'x \equiv b' \pmod{k'} \qquad (2)$$

und umgekehrt überzeugt man sich sogleich, dass jede Wurzel dieser letztern Congruenz auch eine Wurzel der erstern sein wird.

Die beiden Congruenzen (1) und (2) stimmen daher hinsichtlich ihrer Wurzeln vollständig mit einander überein; da nun in der letztern der Coefficient a' relative Primzahl gegen den Modul k' ist, so haben wir wieder den frühern Fall: diese Congruenz ist stets lösbar, und alle ihr genügenden Zahlen bilden in Bezug auf ihren Modul k' nur eine einzige Classe, in der Weise, dass, wenn α eine bestimmte derselben ist, alle andern in der Form

$$x = \alpha + zk' \qquad (3)$$

enthalten sind, wo z jede beliebige ganze Zahl bedeutet. Da nun alle diese Zahlen auch die sämmtlichen Wurzeln der Congruenz (1) bilden, so fragt es sich nur noch, wie viele in Bezug auf den Modul k incongruente Zahlen unter ihnen sich vorfinden. Irgend zwei in der Reihe (3) enthaltene Zahlen $\alpha + zk'$ und $\alpha + z'k'$ werden offenbar stets und auch nur dann congruent in Bezug auf den Modulus k sein, sobald $(z' - z)k'$ durch $k = k'\delta$, und also $z' - z$ durch δ theilbar ist; diese beiden Zahlen werden also einer und derselben Classe, oder verschiedenen Classen in Bezug auf den Modul k angehören, je nachdem die beiden Zahlen z und z' einer und derselben Classe, oder verschiedenen Classen in Bezug auf den Modulus δ angehören; woraus unmittelbar folgt, dass die Reihe (3) sämmtliche Individuen von δ verschiedenen Classen in Bezug auf den Modul k enthält, und es leuchtet ein, dass die folgenden δ Zahlen

$$\alpha,\ \alpha + k',\ \alpha + 2k' \ldots \alpha + (\delta - 1)k'$$

aus jeder dieser δ Classen einen Repräsentanten enthalten. Wir haben mithin folgendes allgemeine Resultat gewonnen:

Damit die Congruenz

$$ax \equiv b \pmod{k}$$

überhaupt Wurzeln besitze, ist erforderlich, dass b durch den grössten gemeinschaftlichen Divisor δ der beiden Zahlen a und k theilbar sei; ist diese Bedingung erfüllt, so hat die Congruenz genau δ incongruente Wurzeln.

Es ist zu bemerken, dass in dem früher behandelten Fall, in welchem $\delta = 1$ ist, die erforderliche Bedingung stets erfüllt ist, ferner, dass dieser Satz auch noch für den Fall $\delta = k$, in welchem also $a \equiv 0 \pmod{k}$ ist, seine Gültigkeit behält, indem, sobald b ebenfalls $\equiv 0 \pmod{k}$ ist, jede beliebige Zahl x dieser identischen Congruenz Genüge leistet.

Um auch ein Beispiel für den allgemeinen Fall zu behandeln, nehmen wir die Congruenz

$$8x \equiv -12 \pmod{60};$$

der grösste gemeinschaftliche Divisor des Coefficienten 8 und des Modul 60 ist hier $= 4$; da die rechte Seite -12 durch denselben theilbar ist, so ist sie möglich und wird 4 nach dem Modul 60 incongruente Wurzeln haben. Wir finden dieselben, indem wir zunächst die Wurzeln der entsprechenden Congruenz

$$2x \equiv -3 \pmod{15}$$

suchen; wir haben oben gesehen, dass dieselben in der Form

$$x \equiv 6 \pmod{15}$$

enthalten sind, und schliessen daraus, dass

$$x \equiv 6, \equiv 21, \equiv 36, \equiv 51 \pmod{60}$$

die vier Wurzeln der ursprünglichen Congruenz sind.

§. 23.

Obgleich im Vorhergehenden das Problem, zu entscheiden, ob eine vorgelegte Congruenz ersten Grades Wurzeln hat oder nicht, und im erstern Fall dieselben aufzufinden, eine vollständige Lösung gefunden hat, so ist dieselbe, sobald der Modul k eine grosse Zahl ist, wegen der erforderlichen Potenzirung für praktische Zwecke nicht wohl anwendbar; wir wollen daher im Folgenden eine einfachere Methode angeben. Offenbar können wir uns auf den Fall beschränken, in welchem der Coefficient der Unbekannten relative Primzahl gegen den Modul ist; ausserdem können wir annehmen, dass die rechte Seite $= 1$ ist; denn um aus der Wurzel einer solchen Congruenz diejenige einer andern zu finden, in welcher die rechte Seite eine andere Zahl ist, genügt es offenbar, dieselbe mit dieser Zahl zu multipliciren. Nennen wir der Bequemlichkeit halber den Modul nicht k, sondern b, so reducirt sich also unsere Aufgabe auf die Auflösung der Congruenz

$$ax \equiv 1 \pmod{b}$$

oder, was dasselbe ist, auf die Auflösung der unbestimmten Gleichung ersten Grades*)

$$ax - by = 1.$$

*) Die erste Lösung dieser Aufgabe findet sich bei *Bachet de Meziriac: Problèmes plaisans et délectables qui se font par les nombres.* 2e éd. 1624.

Wir schicken derselben einige Sätze über einen Algorithmus voraus, der zuerst von *Euler**) behandelt und für die Theorie der Kettenbrüche, sowie auch für unsere spätern Untersuchungen von Wichtigkeit ist. Es seien

$$a, b \tag{1}$$

irgend zwei unbestimmte Grössen, und ebenso

$$\gamma, \delta, \varepsilon \ldots \lambda, \mu, \nu \tag{2}$$

eine Reihe von beliebig vielen unbestimmten Grössen. Aus diesen bilden wir nun successive eine neue Reihe $c, d, e \ldots l, m, n$ nach folgendem Gesetz:

$$\left.\begin{aligned} c &= \gamma b + a \\ d &= \delta c + b \\ e &= \varepsilon d + c \\ &\ldots\ldots \\ n &= \nu m + l \end{aligned}\right\} \tag{3}$$

Substituirt man den Ausdruck für c in den für d, so wird der letztere eine ähnliche Form annehmen wie der erstere, nämlich

$$d = \delta a + (\gamma\delta + 1)b;$$

er besteht also aus einem Gliede, welches den Factor a, und aus einem zweiten, welches den Factor b enthält. Substituirt man nun diesen Ausdruck für d, und den ersten für c in den Ausdruck für e, so nimmt auch dieser letztere dieselbe Form an. So kann man fortfahren, und aus dem Ausdruck für n erkennt man, dass dieses Gesetz allgemein ist; denn sobald l und m schon diese Form erhalten haben, so nimmt auch n dieselbe an. Wir können daher

$$n = Ga + Hb$$

setzen, wo nun G und H unabhängig von a und b sein werden. Man bezeichnet den Coefficienten H, der nur von den in der Reihe (2) befindlichen Grössen abhängt, durch das Zeichen**)

$$[\gamma, \delta, \varepsilon \ldots \lambda, \mu, \nu], \tag{4}$$

und wir werden im Folgenden einige interessante Sätze beweisen, die sich auf dasselbe beziehen.

---

*) *Solutio problematis arithmetici de inveniendo numero, qui per datos numeros divisus, relinquat data residua*, Comm. Ac. Petrop. VII, p. 46. — *De usu novi algorithmi in problemate Pelliano solvendo*, Nov. Comm. Petrop. XI, p. 28. — Vergl. *Gauss: D. A.* art. 27.

**) *Gauss: D. A.* art. 27.

Zunächst leuchtet ein, dass, wenn man mit den Anfangsgliedern

$$b,\ c = \gamma b + a \tag{1'}$$

und der Reihe

$$\delta,\ \varepsilon \ldots \lambda,\ \mu,\ \nu \tag{2'}$$

in derselben Weise verfährt wie oben, man genau dieselben Glieder $d, e \ldots l, m, n$ erhalten wird. Wir können daher gleichzeitig

$$n = Ga + [\gamma, \delta, \varepsilon \ldots \mu, \nu]\, b$$

und

$$n = G'b + [\delta, \varepsilon \ldots \mu, \nu]\, c$$

setzen; ersetzen wir hierin c durch $\gamma b + a$, so erhalten wir

$$n = [\delta, \varepsilon \ldots \mu, \nu]\, a + (\gamma [\delta, \varepsilon \ldots \mu, \nu] + G')\, b,$$

woraus, durch Vergleichung der Coefficienten von a in den beiden Formen für n, zunächst

$$G = [\delta, \varepsilon \ldots \mu, \nu]$$

folgt. Der Coefficient G lässt sich daher durch dasselbe Zeichen ausdrücken wie H. Wir können also von jetzt an schreiben

$$n = [\delta \ldots \mu, \nu]\, a + [\gamma, \delta \ldots \mu, \nu]\, b;$$

da nun auch

$$G' = [\varepsilon \ldots \mu, \nu]$$

sein muss, so erhalten wir durch Vergleichung der Coefficienten von b in den beiden Formen für n den Satz

$$[\gamma, \delta, \varepsilon \ldots \nu] = \gamma [\delta, \varepsilon \ldots \nu] + [\varepsilon \ldots \nu], \tag{5}$$

in welchem das Gesetz ausgedrückt ist, nach welchem die Fortbildung der Ausdrücke von der Form (4) nach links hin geschieht.

Einen ganz analogen Satz für die Fortbildung nach rechts hin erhält man durch die einfache Bemerkung, dass durch die Annahme $a = 0$, $b = 1$ die drei Grössen l, m, n resp. in

$$[\gamma \ldots \lambda],\quad [\gamma \ldots \lambda, \mu],\quad [\gamma \ldots \lambda, \mu, \nu]$$

übergehen, so dass zwischen diesen drei consecutiven Ausdrücken die Relation

$$[\gamma \ldots \lambda, \mu, \nu] = [\gamma \ldots \lambda, \mu]\, \nu + [\gamma \ldots \lambda] \tag{6}$$

besteht.

Verbindet man diese beiden Sätze mit einander, so überzeugt man sich leicht von der Richtigkeit des folgenden:

$$[\nu, \mu \ldots \delta, \gamma] = [\gamma, \delta \ldots \mu, \nu]. \tag{7}$$

Nimmt man nämlich an, dieser Satz sei für alle Ausdrücke dieser Art bewiesen, welche eine kleinere Anzahl von Grössen enthalten, so dass also z. B.

$$[\delta, \varepsilon \ldots \nu] = [\nu \ldots \varepsilon, \delta] \text{ und } [\varepsilon \ldots \nu] = [\nu \ldots \varepsilon],$$

so folgt aus (5):

$$[\gamma, \delta, \varepsilon \ldots \nu] = [\nu \ldots \varepsilon, \delta]\gamma + [\nu \ldots \varepsilon];$$

verbindet man dies mit dem Satz (6), so ergiebt sich unmittelbar die Richtigkeit der Gleichung (7). In der That gilt aber der Satz wirklich für die ersten Fälle; enthält nämlich der Ausdruck nur eine einzige Grösse γ, so versteht sich dies von selbst; und ausserdem ist

$$[\gamma, \delta] = \gamma\delta + 1 = [\delta, \gamma].$$

Hieraus folgt also, dass der Satz auch für jede beliebige Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gilt.

Wir können die Gleichungen (3), durch welche das Bildungsgesetz der Grössen $c, d \ldots n$ ausgedrückt wird, auch in folgender Weise schreiben:

$$\begin{aligned} -c &= (-\gamma)b + (-a) \\ +d &= (-\delta)(-c) + b \\ -e &= (-\varepsilon)d + (-c) \\ &\ldots\ldots\ldots \\ \pm n &= (-\nu)(\mp m) + (\pm l) \end{aligned}$$

wo in der letzten Gleichung das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist. Hieraus geht hervor, dass aus den Anfangsgliedern

$$-a, b \qquad (1'')$$

und der Reihe

$$-\gamma, -\delta, -\varepsilon \ldots -\lambda, -\mu, -\nu \qquad (2'')$$

durch dasselbe frühere Verfahren die Reihe

$$-c, +d, -e \ldots \pm n$$

entsteht. Es wird daher auch

$$\pm n = [-\delta, -\varepsilon \ldots -\nu](-a) + [-\gamma, -\delta, -\varepsilon \ldots -\nu]b$$

und folglich

$$[-\gamma, -\delta \ldots -\nu] = \pm[\gamma, \delta \ldots \nu] \qquad (8)$$

sein, worin wieder das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \nu$ gerade oder ungerade ist.

Endlich kann man die Gleichungen (3) auch in umgekehrter Folge so schreiben:

$$l = (-\nu)m + n$$
$$k = (-\mu)l + m$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$b = (-\delta)c + d$$
$$a = (-\gamma)b + c$$

Es wird daher

$$a = [-\mu \ldots -\gamma]n + [-\nu, -\mu \ldots -\gamma]m$$

oder mit Hülfe des Satzes (8):

$$\pm a = -[\mu \ldots \gamma]n + [\nu, \mu \ldots \gamma]m$$

oder mit Berücksichtigung des Satzes (7):

$$\pm a = -[\gamma, \delta \ldots \mu]n + [\gamma, \delta \ldots \mu, \nu]m.$$

Wenn man nun $a = 1$, $b = 0$ setzt, so gehen m, n resp. in

$$[\delta \ldots \mu], \quad [\delta \ldots \mu, \nu]$$

über, und man erhält das Resultat:

$$[\delta \ldots \mu]\,[\gamma, \delta \ldots \mu, \nu] - [\delta \ldots \mu, \nu]\,[\gamma, \delta \ldots \mu] = \pm 1, \tag{9}$$

wo wieder das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist.

Zum Schluss wollen wir bemerken, dass diese Ausdrücke in der Theorie der Kettenbrüche von der grössten Wichtigkeit sind; bezeichnen wir nämlich einen gewöhnlichen Kettenbruch, in welchem die Zähler sämmtlich $= 1$, und dessen sogenannte Quotienten $\gamma, \delta \ldots \mu, \nu$ sind, kurz durch das Symbol $(\gamma, \delta \ldots \mu, \nu)$, so dass also

$$(\gamma, \delta \ldots \lambda, \mu, \nu) = \gamma + \frac{1}{(\delta \ldots \lambda, \mu, \nu)} = \left(\gamma, \delta \ldots \lambda, \mu + \frac{1}{\nu}\right)$$

ist, so ergiebt sich allgemein durch Reduction desselben

$$(\gamma, \delta \ldots \mu, \nu) = \frac{[\gamma, \delta \ldots \mu, \nu]}{[\delta \ldots \mu, \nu]}. \tag{10}$$

Denn gesetzt, dieser Satz sei schon für jede kleinere Anzahl der Grössen $\gamma, \delta, \varepsilon \ldots \mu, \nu$ bewiesen, so dass also namentlich

$$(\delta, \varepsilon \ldots \mu, \nu) = \frac{[\delta, \varepsilon \ldots \mu, \nu]}{[\varepsilon \ldots \mu, \nu]}$$

ist, so folgt hieraus

$$(\gamma, \delta, \varepsilon \ldots \mu, \nu) = \gamma + \frac{1}{(\delta, \varepsilon \ldots \mu, \nu)}$$
$$= \gamma + \frac{[\varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon \ldots \mu, \nu]} = \frac{\gamma[\delta, \varepsilon \ldots \mu, \nu] + [\varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon \ldots \mu, \nu]}$$

und hieraus ergiebt sich mit Berücksichtigung des Satzes (5) die Gleichung (10). In der That ist aber

$$(\gamma, \delta) = \gamma + \frac{1}{\delta} = \frac{\gamma\delta + 1}{\delta} = \frac{[\gamma, \delta]}{[\delta]};$$

da also der Satz für zwei Grössen γ, δ richtig ist, so ist er auch für jede beliebige Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ richtig.

Sind die Elemente $\gamma, \delta \ldots \mu, \nu$ ganze Zahlen, so gilt dasselbe von den Zählern und Nennern der Brüche

$$\frac{[\gamma]}{1}, \frac{[\gamma, \delta]}{[\delta]} \cdots \frac{[\gamma, \delta \ldots \mu, \nu]}{[\delta \ldots \mu, \nu]};$$

ferner ist jeder dieser Brüche irreductibel, d. h. durch die kleinsten Zahlen ausgedrückt; denn es folgt z. B. aus der Relation (9), dass Zähler und Nenner des letzten der obigen Brüche ohne gemeinschaftlichen Divisor sind.

§. 24.

Die vorstehenden Sätze, welche eigentlich in die Theorie der Differenzen-Gleichungen zweiter Ordnung*) gehören, sind deshalb gleich in solcher Vollständigkeit aufgestellt, damit wir bei einer spätern Untersuchung nicht nöthig haben, von Neuem auf denselben Algorithmus zurückzukommen; für unsern nächsten Bedarf, nämlich für die Lösung der unbestimmten Gleichung

$$ax - by = 1,$$

in welcher wir nun wieder a und b als zwei gegebene relative Primzahlen ansehen, genügt schon ein kleiner Theil der vorhergehenden Resultate. Zu dem Zweck verfahren wir nun, wie es bei der Aufsuchung des grössten gemeinschaftlichen Divisors der beiden Zahlen (oder bei der Verwandlung des Bruches $a:b$ in einen Kettenbruch) geschieht, indem wir das System der folgenden Gleichungen bilden

$$\begin{aligned} a &= \gamma b + c \\ b &= \delta c + d \\ &\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ l &= \nu m + 1 \end{aligned}$$

wobei zuletzt der Rest 1 auftreten muss (§. 5); diese Gleichungen können wir auch so schreiben

*) Vergl. *Jacobi: Allgemeine Theorie der kettenbruchähnlichen Algorithmen, in welchen jede Zahl aus Drei vorhergehenden gebildet wird,* Crelle's Journal Bd. LXIX.

$$c = (-\gamma) b + a$$
$$d = (-\delta) c + b$$
$$\ldots\ldots$$
$$1 = (-\nu) m + l$$

und hieraus folgt, dass

$$1 = [-\delta, -\varepsilon \cdots -\mu, -\nu] a + [-\gamma, -\delta, -\varepsilon \cdots -\mu, -\nu] b$$

oder nach §. 23, (8)

$$1 = \mp [\delta, \varepsilon \ldots \mu, \nu] a \pm [\gamma, \delta, \varepsilon \ldots \mu, \nu] b$$

ist, worin das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist. Wir erhalten daher folgende Auflösung der unbestimmten Gleichung:

$$x = \mp [\delta, \varepsilon \ldots \mu, \nu], \quad y = \mp [\gamma, \delta, \varepsilon \ldots \mu, \nu].$$

Hiermit ist also auch eine Wurzel x der Congruenz

$$a x \equiv 1 \pmod{b}$$

gefunden, und dies genügt vollständig, da alle anderen dieser einen nach dem Modul b congruent sind*).

Wenden wir diese Methode auf unser Beispiel

$$2 x \equiv 1 \pmod{15}$$

an, so erhalten wir

$$2 = 0 \,.\, 15 + 2, \quad 15 = 7 \,.\, 2 + 1$$

also

$$\gamma = 0, \; \delta = 7, \quad x \equiv -[\delta] \equiv -7 \equiv 8 \pmod{15}$$

und hieraus folgt, dass

$$x \equiv -7 \,.\, (-3) \equiv 21 \equiv 6 \pmod{15}$$

die Wurzel der Congruenz

$$2 x \equiv -3 \pmod{15}$$

ist.

Als zweites Beispiel wählen wir die Congruenz

$$37 x \equiv 1 \pmod{100};$$

indem wir ebenso verfahren, erhalten wir

$$37 = 0 \,.\, 100 + 37; \quad 100 = 2 \,.\, 37 + 26; \quad 37 = 1 \,.\, 26 + 11;$$
$$26 = 2 \,.\, 11 + 4; \quad 11 = 2 \,.\, 4 + 3; \quad 4 = 1 \,.\, 3 + 1$$

*) Man überzeugt sich leicht, dass aus einer Lösung x_0, y_0 alle anderen sich durch die Gleichungen $x = x_0 + bz$, $y = y_0 + az$ ableiten lassen, wo z eine willkürliche ganze Zahl bedeutet. Vergl. §. 60.

und also

$$x \equiv -[2, 1, 2, 2, 1] \pmod{100}.$$

Nun ist, wenn wir von rechts nach links rechnen,

$$[1] = 1, [2, 1] = 3, [2, 2, 1] = 7, [1, 2, 2, 1] = 10,$$
$$[2, 1, 2, 2, 1] = 27,$$

also

$$x \equiv -27 \equiv 73 \pmod{100}.$$

Da $\varphi(100) = \varphi(4)\,\varphi(25) = 2 \,.\, 20 = 40$ ist, so hätten wir nach unserer früheren Methode die Auflösung

$$x \equiv 37^{39} \pmod{100}$$

erhalten; die hierin angedeutete Rechnung würde sich zwar durch einige Kunstgriffe bedeutend abkürzen lassen, allein doch viel langwieriger sein als die nach der zweiten Methode ausgeführte Rechnung.

Kommt es darauf an, auch den Werth von

$$y = \mp[\gamma, \delta, \varepsilon \ldots \mu, \nu]$$

zu berechnen, so ist es vortheilhaft, die Berechnung des Werthes

$$x = \mp[\delta, \varepsilon \ldots \mu, \nu]$$

von rechts nach links vorzunehmen; man findet dann nach der Formel (5) des §. 23 aus

$$[\varepsilon \ldots \mu, \nu] \text{ und } [\delta, \varepsilon \ldots \mu, \nu]$$

unmittelbar den Werth von y. So oft $\gamma = 0$, also $a < b$ ist, reducirt sich y auf

$$y = \mp[\varepsilon \ldots \mu, \nu].$$

Dies ist in unseren Beispielen der Fall; in dem zweiten erhält man auf diese Weise

$$y = -[0, 2, 1, 2, 2, 1] = -[1, 2, 2, 1] = -10,$$

und in der That ist

$$37 \,.\, (-27) - 100 \,.\, (-10) = 1.$$

Bei dieser Lösung der unbestimmten Gleichung $ax - by = 1$ in ganzen Zahlen x, y war stillschweigend vorausgesetzt, dass die beiden gegebenen relativen Primzahlen a, b *positive* Zahlen sind; doch erkennt man leicht, dass hierdurch die Allgemeinheit der Lösung nicht beeinträchtigt wird.

Wir bemerken ferner, dass durch wiederholte Anwendung desselben Verfahrens folgende allgemeinere Aufgabe gelöst werden kann: *Sind a, b, c ... gegebene ganze Zahlen, deren grösster ge-*

meinschaftlicher Divisor m *ist, so sollen ebensoviele ganze Zahlen* $x, y, z \ldots$ *gefunden werden, welche der Gleichung*

$$ax + by + cz + \cdots = m$$

genügen. Denn gesetzt, man habe für die Zahlen $b, c \ldots$, deren grösster gemeinschaftlicher Divisor m' nothwendig ein Multiplum von m ist, schon ganze Zahlen $y', z' \ldots$ gefunden, welche der Bedingung

$$by' + cz' + \cdots = m'$$

genügen, so löse man, da m der grösste gemeinschaftliche Divisor von a und m' ist, nach der obigen Methode die Gleichung

$$ax + m'x' = m$$

in ganzen Zahlen x, x', so wird die vorgelegte Gleichung durch die Zahlen x, $y = x'y'$, $z = x'z' \ldots$ befriedigt.

§. 25.

Auf das im Vorhergehenden behandelte Problem der Auflösung der Congruenzen ersten Grades lässt sich das folgende zurückführen:

Alle Zahlen x *zu finden, welche in Bezug auf zwei gegebene Moduln* a, b *gegebenen Zahlen resp.* α, β *congruent sind, d. h. welche den beiden Forderungen*

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}$$

genügen.

Da nämlich alle Zahlen x, welche die erste dieser beiden Forderungen erfüllen, in der Form $x = \alpha + at$ enthalten sind, wo t jede beliebige ganze Zahl bedeutet, so kommt es nur noch darauf an, dieses t näher so zu bestimmen, dass

$$at \equiv \beta - \alpha \pmod{b} \tag{1}$$

wird. Bezeichnet man nun mit δ den grössten gemeinschaftlichen Divisor der beiden Moduln a und b, so muss, wenn diese Congruenz möglich sein soll, $\beta - \alpha$ durch δ theilbar, d. h. es muss

$$\alpha \equiv \beta \pmod{\delta} \tag{2}$$

sein. Ist diese Bedingung nicht erfüllt, so existirt keine Zahl, welche der Aufgabe genügt; ist sie aber erfüllt, so sind sämmtliche der Congruenz (1) genügende Zahlen t in der Form

$$t \equiv \gamma \left(\text{mod.}\ \frac{b}{\delta}\right) \text{ oder } t = \gamma + \frac{b}{\delta} u$$

enthalten, wo γ eine bestimmte von ihnen, und u jede beliebige ganze Zahl bedeutet. Hieraus folgt, dass die gesuchten Zahlen durch die Formel

$$x = \alpha + \gamma a + \frac{ab}{\delta} u \text{ oder } x \equiv x_0 \left(\text{mod.}\ \frac{ab}{\delta}\right)$$

gegeben werden, wo $x_0 = \alpha + \gamma a$ selbst eine der gesuchten Zahlen, und der Modulus offenbar das kleinste gemeinschaftliche Multiplum der beiden gegebenen Moduln a, b ist.

Werden z. B. die Zahlen gesucht, welche durch 12 dividirt den Rest 7, durch 15 dividirt den Rest 4 lassen, so hat man die Congruenzen

$$x \equiv 7 \ (\text{mod.}\ 12), \quad x \equiv 4 \ (\text{mod.}\ 15).$$

Man setzt also $x = 7 + 12t$, und erhält für t die Congruenz

$$12t \equiv -3 \ (\text{mod.}\ 15),$$

welche (da hier die Bedingung (2) erfüllt ist) sich auf

$$4t \equiv -1 \ (\text{mod.}\ 5)$$

reducirt. Hieraus folgt

$$t \equiv 1 \ (\text{mod.}\ 5)$$

und also

$$x = 7 + 12t \equiv 19 \ (\text{mod.}\ 60).$$

Besonders bemerkenswerth ist der besondere Fall, in welchem die beiden gegebenen Moduln a, b relative Primzahlen sind; da gleichzeitig $\delta = 1$ wird, so fällt die Bedingung (2) ganz fort; die Auflösung ist stets möglich und liefert ein Resultat von der Form

$$x \equiv x_0 \ (\text{mod.}\ ab).$$

Die ursprüngliche Aufgabe lässt sich auch leicht für den Fall verallgemeinern, in welchem eine Reihe von beliebig vielen Moduln und eine Reihe ihnen entsprechender Reste gegeben ist; für uns ist indessen nur der Fall von Wichtigkeit, in welchem die gegebenen Moduln $a, b, c \ldots$ relative Primzahlen sind; wir beschränken uns daher auf denselben, und stellen uns unter dieser Voraussetzung die Aufgabe, alle Zahlen x zu finden, welche dem System von Congruenzen

$$x \equiv \alpha \ (\text{mod.}\ a), \quad x \equiv \beta \ (\text{mod.}\ b), \quad x \equiv \gamma \ (\text{mod.}\ c) \ldots$$

genügen. Da wir nun schon wissen, dass alle Zahlen, welche die beiden ersten dieser Forderungen erfüllen, in der Form $x \equiv \beta_1$ (mod. ab)

enthalten sind, wo die Zahl β_1 nach dem Vorhergehenden gefunden werden kann, so kommt unsere Aufgabe offenbar auf die einfachere zurück, alle Zahlen x zu finden, welche dem folgenden System von Congruenzen genügen:

$$x \equiv \beta_1 \pmod{ab}, \quad x \equiv \gamma \pmod{c} \ldots$$

Da nun der Modul ab der ersten dieser Congruenzen wieder relative Primzahl gegen jeden folgenden Modul $c \ldots$ ist, so kann man in derselben Weise fortfahren und gelangt so zu dem Resultat, dass sämmtliche Zahlen x in der Form

$$x \equiv x_0 \pmod{m}$$

enthalten sind, wo x_0 eine bestimmte von ihnen, und m das Product $abc \ldots$ aus allen gegebenen Moduln bedeutet.

Statt eine solche Zahl x_0 in der eben angegebenen Weise durch successive Auflösung einer Reihe von Congruenzen ersten Grades in Bezug auf die Moduln $b, c \ldots$ zu suchen, kann man auch auf folgende Art symmetrisch verfahren.

Man setze $m = aA = bB = cC \ldots$ und bestimme (nach §. 24) zunächst Zahlen $a', b', c' \ldots$, welche den Congruenzen

$$Aa' \equiv 1 \pmod{a}, \quad Bb' \equiv 1 \pmod{b}, \quad Cc' \equiv 1 \pmod{c} \ldots$$

genügen; so wird

$$x \equiv Aa'\alpha + Bb'\beta + Cc'\gamma + \cdots \pmod{m};$$

denn da $B, C \ldots$ durch a theilbar sind, so ist $x \equiv Aa'\alpha \equiv \alpha \pmod{a}$, und ebenso $\equiv \beta \pmod{b}$, $\equiv \gamma \pmod{c}$ u. s. w.

Ein besonderer Vortheil dieser Methode besteht darin, dass die Hülfszahlen $a', b', c' \ldots$ ganz unabhängig von $\alpha, \beta, \gamma \ldots$ sind, und daher stets dieselben bleiben, wie auch die letzteren variiren mögen, vorausgesetzt natürlich, dass das System der Moduln $a, b, c \ldots$ unverändert bleibt.

Es folgt ferner hieraus, dass x ein vollständiges Restsystem nach dem Modul m durchläuft, sobald die Reste $\alpha, \beta, \gamma \ldots$ vollständige Restsysteme resp. in Bezug auf die Moduln $a, b, c \ldots$ durchlaufen; denn wenn $\alpha', \beta', \gamma' \ldots$ irgend ein zweites System gegebener Reste ist, so wird

$$Aa'\alpha' + Bb'\beta' + Cc'\gamma' + \cdots$$

stets und nur dann

$$\equiv Aa'\alpha + Bb'\beta + Cc'\gamma + \cdots$$

nach dem Modulus m sein, wenn gleichzeitig

$$\alpha' \equiv \alpha \pmod{a}, \quad \beta' \equiv \beta \pmod{b}, \quad \gamma' \equiv \gamma \pmod{c}$$

u. s. w. ist; da ferner $\alpha, \beta, \gamma \ldots$ resp. $a, b, c \ldots$ verschiedene Werthe durchlaufen, so ist die Anzahl aller verschiedenen Restsysteme, also auch die Anzahl der resultirenden nach dem Modul m incongruenten Werthe von x gleich $abc \ldots = m$; d. h. x durchläuft ein vollständiges Restsystem nach dem Modul m.

Ist ferner α relative Primzahl zu a, β zu b u. s. f., so ist x auch relative Primzahl zu m, und umgekehrt; hieraus folgt leicht ein neuer Beweis des Satzes, dass $\varphi(ab) = \varphi(a)\,\varphi(b)$ ist.

Endlich ergiebt sich, dass, wenn x irgend eine ganze Zahl bedeutet, stets

$$\frac{x}{m} = h + \frac{u}{a} + \frac{v}{b} + \frac{w}{c} + \cdots$$

gesetzt werden kann, wo $h, u, v, w \ldots$ ganze Zahlen bedeuten. Denn lässt x in Bezug auf die Moduln $a, b, c \ldots$ resp. die Reste $\alpha, \beta, \gamma \ldots$, so ist nach dem Obigen

$$x = hm + Aa'\alpha + Bb'\beta + Cc'\gamma + \cdots,$$

wo h eine ganze Zahl bedeutet, und folglich

$$\frac{x}{m} = h + \frac{a'\alpha}{a} + \frac{b'\beta}{b} + \frac{c'\gamma}{c} + \cdots$$

§. 26.

Wir wenden uns nun zu der Betrachtung der Congruenzen höherer Grade, beschränken uns aber dabei auf den einfachsten Fall, in welchem der Modul p eine *Primzahl* ist. Die allgemeinste Form einer Congruenz $n$ten Grades ist die folgende:

$$ax^n + bx^{n-1} + cx^{n-2} + \cdots + h \equiv 0 \pmod{p},$$

in welcher der höchste Coefficient a als nicht theilbar durch die Primzahl p vorausgesetzt wird. Ebenso wie man jede Gleichung leicht auf den Fall zurückführen kann, in welchem der höchste Coefficient $= 1$ ist, so erreicht man auch hier dasselbe, wenn man die Congruenz mit einer Zahl a' multiplicirt, welche der Bedingung $aa' \equiv 1 \pmod{p}$ genügt und also eine Wurzel der stets lösbaren Congruenz $ax \equiv 1 \pmod{p}$ ist. Doch hängt hiervon die Gültigkeit der folgenden Sätze nicht im Mindesten ab.

Wir bezeichnen der Einfachheit halber das auf der linken Seite der obigen Congruenz befindliche Polynom $n$ten Grades kurz mit $f(x)$. Hat nun eine solche Congruenz

$$f(x) \equiv 0 \pmod{p} \qquad (1)$$

eine Wurzel $x \equiv \alpha$ und dividirt man $f(x)$ durch $x - \alpha$, so wird der Divisionsrest r_1 eine durch p theilbare Zahl sein; denn bezeichnet man den Quotienten der Division, welcher eine ganze Function vom $(n-1)$ten Grade mit ganzzahligen Coefficienten ist, mit $f_1(x)$, so ist

$$f(x) = (x - \alpha) f_1(x) + r_1 \qquad (2)$$

und hierin ist $r_1 = f(\alpha)$ der Voraussetzung nach $\equiv 0 \pmod{p}$.

Hat nun die Congruenz (1) noch eine zweite von α verschiedene, d. h. nicht mit α congruente Wurzel β, so folgt aus (2), dass

$$(\beta - \alpha) f_1(\beta) \equiv 0 \pmod{p}$$

und also, da $\beta - \alpha$ nicht durch p theilbar ist, dass $f_1(\beta) \equiv 0$, d. h. dass β eine Wurzel der Congruenz $f_1(x) \equiv 0 \pmod{p}$ sein muss. Man kann daher wieder

$$f_1(x) = (x - \beta) f_2(x) + r_2$$

setzen, wo der Rest r_2 wieder eine durch p theilbare Zahl, und der Quotient $f_2(x)$ eine ganze Function $(n-2)$ten Grades mit ganzzahligen Coefficienten ist. Setzt man aber diesen Ausdruck für $f_1(x)$ in die Gleichung (2) ein, so nimmt dieselbe die Form

$$f(x) = (x - \alpha)(x - \beta) f_2(x) + r_2(x - \alpha) + r_1$$

oder, da r_1 und r_2 durch p theilbar sind, die Form

$$f(x) = (x - \alpha)(x - \beta) f_2(x) + p(lx + m)$$

an, in welcher l und m ganze Zahlen sind.

Besitzt nun die Congruenz (1) noch eine dritte von α und β verschiedene Wurzel γ, so ergiebt sich, da weder $(\gamma - \alpha)$ noch $(\gamma - \beta)$ durch p theilbar ist, dass γ eine Wurzel der Congruenz $f_2(x) \equiv 0$ ist; verfährt man daher wie früher, so erhält man eine Gleichung von der Form

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma) f_3(x) + p(rx^2 + sx + t),$$

wo r, s, t ganze Zahlen bedeuten. Setzt man diese Schlussweise fort, so gelangt man offenbar zu folgendem Satze: *Besitzt die Congruenz nten Grades*

$$f(x) \equiv 0 \pmod{p},$$

deren Modulus p eine Primzahl ist, n incongruente Wurzeln $\alpha, \beta, \gamma \ldots \lambda$, *so ist ihre linke Seite von der Form*

$$f(x) = a(x - \alpha)(x - \beta)(x - \gamma) \ldots (x - \lambda) + p\psi(x), \qquad (3)$$

wo a den höchsten Coefficienten von $f(x)$, und $\psi(x)$ ein Polynom bedeutet, dessen Coefficienten ganze Zahlen sind.

Und aus diesem ersten Satze folgt sogleich der zweite*): *Eine Congruenz vom Grade n, deren Modulus eine Primzahl ist, kann niemals mehr als n incongruente Wurzeln haben.* Denn hätte die Congruenz (1) ausser den n Wurzeln $\alpha, \beta \ldots \lambda$ noch mindestens eine solche μ, die mit keiner der vorhergehenden congruent ist, so würde aus der Gleichung (3) folgen, dass das Product

$$a(\mu-\alpha)\,(\mu-\beta)\,(\mu-\gamma)\ldots(\mu-\lambda)$$

durch p theilbar wäre, was unmöglich ist, da der Voraussetzung nach keiner der Factoren durch p theilbar ist.

Man hätte diese beiden Sätze, welche für die Folge von der grössten Wichtigkeit sind, auch in umgekehrter Folge aus dem in der Gleichung (2) ausgesprochenen Resultat schliessen können. Da nämlich jede von α verschiedene Wurzel β der Congruenz (1) eine Wurzel der Congruenz nächst niedrigern Grades

$$f_1(x) \equiv 0 \pmod{p}$$

ist, so folgt hieraus unmittelbar, dass die erstere Congruenz höchstens eine Wurzel mehr besitzt, als die letztere; da nun eine Congruenz ersten Grades (sobald der Modulus eine Primzahl ist) nur eine Wurzel besitzt, so kann eine Congruenz vom zweiten Grade höchstens 2, folglich eine Congruenz dritten Grades höchstens 3 u. s. f., allgemein eine Congruenz $n$ten Grades höchstens n incongruente Wurzeln besitzen. Und nachdem so der zweite Satz bewiesen ist, ergiebt sich auch der erste leicht auf folgende Weise. Gesetzt, die Congruenz (1) vom $n$ten Grade hat wirklich n incongruente Wurzeln $\alpha, \beta, \gamma \ldots \lambda$, so bilde man die Differenz

$$f(x)-a(x-\alpha)\,(x-\beta)\,(x-\gamma)\ldots(x-\lambda)=\varphi(x)$$

wo a den höchsten Coefficienten in $f(x)$ bezeichnet, und denke sich dieselbe nach Potenzen von x geordnet; dann ist zu zeigen, dass alle Coefficienten dieses Polynoms $\varphi(x)$, dessen Grad höchstens $= n-1$, also jedenfalls kleiner als n ist, durch p theilbar sind. Gesetzt, dies wäre nicht der Fall, und es wäre x^r die höchste in $\varphi(x)$ vorkommende Potenz von x, deren Coefficient nicht durch p theilbar wäre, so wäre

$$\varphi(x) \equiv 0 \pmod{p}$$

---

*) *Lagrange: Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers,* Mém. de l'Ac. de Berlin. T. XXIV.

eine Congruenz vom $r$ten Grade, welche, wie man unmittelbar einsieht, die n incongruenten Zahlen $\alpha, \beta \ldots \lambda$ zu Wurzeln hätte, also, da $r < n$ ist, mehr Wurzeln besässe, als ihr Grad Einheiten enthält. Da dies gegen den schon bewiesenen Satz streitet, so müssen wirklich alle Coefficienten von $\varphi(x)$ durch p theilbar sein, d. h. es muss

$$\varphi(x) = p\,\psi(x)$$

sein, wo sämmtliche Coefficienten des Polynoms $\psi(x)$ ganze Zahlen sind. Dies war aber der Inhalt des ersten Satzes.

Wir können zu diesen beiden Sätzen noch den folgenden dritten hinzufügen: *Wenn*

$$f(x) = \varphi(x)\,\psi(x)$$

ist, wo die Coefficienten der Polynome $\varphi(x)$ und $\psi(x)$ sämmtlich ganze Zahlen sind, und wenn die Congruenz

$$f(x) \equiv 0 \pmod{p}, \tag{4}$$

(wo p wieder eine Primzahl bedeutet) ebenso viele incongruente Wurzeln besitzt, als ihr Grad Einheiten enthält, so gilt dasselbe von jeder der beiden Congruenzen

$$\varphi(x) \equiv 0 \pmod{p}, \quad \psi(x) \equiv 0 \pmod{p}. \tag{5}$$

Zunächst leuchtet nämlich ein, dass jede Wurzel α der Congruenz (4) auch eine Wurzel von mindestens einer der beiden Congruenzen (5) sein muss; denn aus

$$\varphi(\alpha)\,\psi(\alpha) = f(\alpha) \equiv 0 \pmod{p}$$

folgt, dass mindestens eine der beiden Zahlen $\varphi(\alpha)$, $\psi(\alpha)$ durch p theilbar sein muss. Hätte nun eine der beiden Congruenzen (5) weniger incongruente Wurzeln als ihr Grad Einheiten enthält, so müsste nothwendig die Anzahl der Wurzeln der andern Congruenz d. h. der übrigen Wurzeln der Congruenz (4) ihren Grad übersteigen, da die Summe der Grade der beiden Polynome $\varphi(x)$ und $\psi(x)$ genau dem Grade des Polynoms $f(x)$ gleich ist. Da dies gegen den zweiten Satz verstossen würde, so muss die Anzahl der incongruenten Wurzeln einer jeden der beiden Congruenzen (5) genau ihrem Grade gleich sein *).

---

*) Eine weitere Entwicklung dieses Gegenstandes findet man in des Herausgebers Abhandlung: *Abriss einer Theorie der höheren Congruenzen in Bezug auf einen reellen Primzahl-Modulus*, Crelle's Journal Bd. LIV. — Vergl. die nachgelassene Abhandlung von *Gauss: Analysis Residuorum*, Gauss' Werke Bd. II. 1863.

§. 27.

Von diesen wichtigen Sätzen machen wir sogleich eine Anwendung. Zufolge des Fermat'schen Satzes genügt jede der $(p-1)$ unter einander nach dem Modul p incongruenten Zahlen

$$1, 2, 3 \ldots (p-1)$$

der Congruenz

$$x^{p-1} - 1 \equiv 0 \pmod{p},$$

und diese Zahlen bilden auch ihre sämmtlichen incongruenten Wurzeln. Es ist daher nach dem ersten der vorhergehenden drei Sätze

$$x^{p-1} - 1 = (x-1)(x-2)(x-3) \ldots (x-p+1) + p\,\psi(x),$$

worin $\psi(x)$ ein Polynom mit ganzen Coefficienten bezeichnet. Entwickelt man daher das rechter Hand befindliche Product nach Potenzen von x, so muss der Coefficient einer jeden Potenz von x dem entsprechenden linker Hand in Bezug auf den Modul p congruent sein. Wir wollen hier nur den interessantesten Fall betrachten der sich durch die Vergleichung der Glieder ergiebt, welche von x unabhängig sind. Ist zunächst p eine *ungerade* Primzahl, so ist dieses Glied rechter Hand, da die Anzahl $p-1$ der negativen Factoren gerade ist,

$$= 1 \,.\, 2 \,.\, 3 \ldots (p-1),$$

linker Hand dagegen $= -1$, und hieraus ergiebt sich der nach *Wilson* benannte Satz:

Wenn p eine Primzahl bedeutet, so ist das um eine Einheit vergrösserte Product aller kleineren Zahlen als p durch p theilbar in Zeichen

$$1 \,.\, 2 \ldots (p-1) \equiv -1 \pmod{p}.$$

So ist z. B.

$$1 \,.\, 2 \,.\, 3 \,.\, 4 \,.\, 5 \,.\, 6 + 1 = 721$$

theilbar durch 7.

Der Wilson'sche Satz gilt aber auch für die Primzahl 2, da in diesem Fall $+1$ und -1 einander congruent sind.

Dieser Satz ist dadurch bemerkenswerth, dass er sich umkehren lässt und deshalb ein charakteristisches Merkmal für eine Primzahl abgiebt. Denn nimmt man umgekehrt an, es sei

$$1 \,.\, 2 \,.\, 3 \ldots (p-1)+1$$

durch p theilbar, so muss p eine Primzahl sein; wäre nämlich p eine zusammengesetzte Zahl, also ausser durch 1 und durch sich selbst auch noch durch eine andere Zahl a theilbar, so würde a nothwendig eine der Zahlen $2, 3 \ldots (p-1)$ sein müssen; da nun die obige Summe und ihr erstes Glied durch a theilbar ist, so müsste auch das zweite Glied 1 durch a theilbar sein, was nicht möglich ist.

Einen andern interessanten Satz erhält man durch Anwendung des dritten der vorhergehenden Sätze auf dasselbe Beispiel. Bezeichnet nämlich δ irgend einen Divisor von $p-1$, so ist bekanntlich

$$x^{p-1} - 1 = (x^{\delta} - 1)\, \psi(x),$$

wo $\psi(x)$ ein Polynom mit ganzen Coefficienten bedeutet. Hieraus folgt also: *Die Congruenz*

$$x^{\delta} \equiv 1 \pmod{p},$$

deren Grad δ ein Divisor von $p-1$ ist, besitzt stets δ incongruente Wurzeln.

§. 28.

Der zuletzt abgeleitete Satz gehört seinem Inhalte nach eigentlich in eine allgemeinere Theorie, nämlich in die Theorie der *binomischen Congruenzen* von der Form

$$a x^n \equiv b \pmod{k}.$$

Dieselbe stützt sich auf die Betrachtung der sogenannten *Potenzreste*, d. h. der Reste der successiven Potenzen einer Zahl, und wir beschäftigen uns daher zunächst mit der Untersuchung der interessanten Gesetze, welche hier hervortreten.

Es sei also k ein beliebiger Modul, und a relative Primzahl gegen denselben; bilden wir nun die Reihe

$$1, a, a^2, a^3 \ldots$$

der successiven Potenzen von a und setzen dieselbe hinreichend weit fort, so muss es einmal geschehen, dass zwei verschiedene Glieder a^s und a^{s+n} einander nach dem Modul k congruent werden; denn es giebt ja nur eine endliche Anzahl incongruenter Zahlen. Aus der Congruenz

$$a^{s+n} = a^s \cdot a^n \equiv a^s \pmod{k}$$

folgt aber, da a^s relative Primzahl gegen den Modul k ist, dass

$$a^n \equiv 1 \pmod{k}$$

ist. Es giebt daher, was wir auch schon durch den verallgemeinerten Fermat'schen Satz (§. 19) wussten, stets eine Potenz von a, welche durch k dividirt den Rest 1 lässt. Unter allen Potenzen von a, welche dieselbe Eigenschaft haben, ist aber besonders diejenige bemerkenswerth, welche den kleinsten Exponenten hat; doch versteht sich von selbst, dass der Exponent Null hier nicht in Betracht kommt, für welchen die entsprechende Potenz ja stets $\equiv 1$ sein würde. Bezeichnen wir mit δ diesen kleinsten positiven Exponenten, für welchen

$$a^\delta \equiv 1 \pmod{k}$$

wird, so wollen wir sagen, die Zahl a *gehöre* zu dem Exponenten δ oder zu der Zahl δ. Dann leuchtet zunächst ein, dass die ersten δ Glieder der obigen Potenzreihe, d. h. die Zahlen

$$1, \quad a, \quad a^2 \ldots a^{\delta-1}$$

sämmtlich incongruent unter einander sind; denn aus einer Congruenz von der Form $a^{s+n} \equiv a^s$, wo s und $s+n$ kleiner als δ sind, würde wieder $a^n \equiv 1$ folgen, was mit der Voraussetzung im Widerspruch steht, dass keine niedrigere Potenz als a^δ den Rest 1 lässt.

Die folgenden Glieder der Reihe geben nun genau dieselben Reste, und auch in derselben Reihenfolge, denn es ist

$$\begin{array}{llll} a^\delta \equiv 1, & a^{\delta+1} \equiv a, & a^{\delta+2} \equiv a^2 \ldots & a^{2\delta-1} \equiv a^{\delta-1} \\ a^{2\delta} \equiv 1, & a^{2\delta+1} \equiv a, & a^{2\delta+2} \equiv a^2 \ldots & a^{3\delta-1} \equiv a^{\delta-1} \\ a^{3\delta} \equiv 1, & a^{3\delta+1} \equiv a, & a^{3\delta+2} \equiv a^2 \ldots & a^{4\delta-1} \equiv a^{\delta-1} \end{array}$$

u. s. w.

Um daher zu erfahren, welchen Rest eine beliebige Potenz a^s lässt, dividire man den Exponenten s durch δ und bringe dadurch s in die Form $s = m\delta + r$, wo r eine der Zahlen $0, 1, 2 \ldots (\delta - 1)$ bezeichnet. Dann ist

$$a^s = a^{m\delta+r} \equiv a^r \pmod{k}.$$

Hieraus geht ferner hervor, dass zwei solche Potenzen wie a^s und $a^{s'}$ stets, aber auch nur dann congruent sein werden in Bezug auf den Modul k, wenn $s \equiv s' \pmod{\delta}$; denn ist r' der bei der Division von s' durch δ hervorgehende Rest, so ist $a^{s'} \equiv a^{r'} \pmod{k}$. Ist daher

$$a^s \equiv a^{s'} \pmod{k}$$

so muss auch

$$a^r \equiv a^{r'} \pmod{k}$$

sein; da aber r und r' kleiner als δ sind, so ist dies nur dann möglich, wenn $r = r'$ ist, woraus $s \equiv s' \pmod{\delta}$ folgt; und umgekehrt leuchtet ein, dass, sobald $s \equiv s' \pmod{\delta}$, also $r = r'$ ist, auch $a^s \equiv a^{s'} \pmod{k}$ sein muss.

Ein specieller Fall ist der, dass, sobald $a^s \equiv 1$, also $a^s \equiv a^0$ ist, nothwendig $s \equiv 0 \pmod{\delta}$, d. h. dass s theilbar durch δ sein muss. Nun wissen wir schon aus dem verallgemeinerten Fermat'schen Satz, dass stets

$$a^{\varphi(k)} \equiv 1 \pmod{k}$$

ist; hieraus folgt also, dass die Zahl δ, zu welcher eine Zahl a gehört, stets ein Divisor von $\varphi(k)$ sein muss *).

§. 29.

Beschränken wir uns jetzt wieder auf den Fall, in welchem der Modul eine Primzahl p und also a irgend eine durch p nicht theilbare Zahl ist, so folgt aus der letzten Bemerkung, dass die Zahl δ, zu welcher a gehört, jedenfalls ein Divisor von $\varphi(p) = p - 1$ sein muss. Man kann nun umgekehrt fragen: wenn δ irgend ein Divisor von $p - 1$ ist, giebt es dann jedesmal auch Zahlen a, welche zu δ gehören? und wie viele? Nehmen wir zunächst einmal ein Beispiel, indem wir $p = 7$ setzen. Da aus $a \equiv a' \pmod{p}$ auch stets $a^s \equiv a'^s \pmod{p}$ folgt, so gehören je zwei congruente Zahlen auch stets zu demselben Exponenten, und wir brauchen daher in unserm Beispiel nur die Zahlen $a = 1, 2, 3, 4, 5, 6$ zu betrachten; durch wirkliches Potenziren, welches man dadurch abkürzt, dass man statt jeder Potenz immer ihren kleinsten Rest substituirt, findet man nun das in der folgenden Tabelle ausgedrückte Resultat:

a	1	2	3	4	5	6
δ	1	3	6	3	6	2

Es gehört daher zu dem Divisor $\delta = 1$ nur die einzige Zahl 1, zu $\delta = 2$ nur die einzige Zahl 6; zu $\delta = 3$ gehören zwei Zah-

*) Ein anderer Beweis dieses Satzes findet sich in den Supplementen V. §. 127.

len, nämlich 2 und 4, und zu $\delta = 6$ gehören die beiden Zahlen 3 und 5.

Nehmen wir nun vorläufig einmal an, dass *mindestens eine* Zahl a existirt, welche zu dem Exponenten δ gehört, so sind die δ Zahlen

$$1,\ a,\ a^2 \ldots a^{\delta-1} \qquad (A)$$

nach dem Vorhergehenden sämmtlich incongruent; da ferner $a^\delta \equiv 1$, so ist auch

$$(a^r)^\delta = (a^\delta)^r \equiv 1 \text{ (mod. } p),$$

d. h. die δ Zahlen (A) sind Wurzeln der Congruenz

$$x^\delta \equiv 1 \text{ (mod. } p),$$

und da sie unter einander incongruent sind, und der Modulus eine Primzahl ist, so bilden sie auch die sämmtlichen Wurzeln dieser Congruenz vom Grade δ. Jede Zahl aber, welche zum Exponenten δ gehört, muss vor Allem eine Wurzel dieser Congruenz sein, und wir haben daher alle etwa existirenden Zahlen, die zu δ gehören, unter den Zahlen (A) zu suchen. Wir fragen daher: zu welchem Exponenten h gehört irgend eine dieser Zahlen, z. B. a^r? d. h. welches ist die kleinste positive Zahl h, für welche

$$(a^r)^h = a^{rh} \equiv 1 \text{ (mod. } p)$$

ist? Offenbar muss rh (da a zum Exponenten δ gehört) durch δ theilbar sein; ist daher ε der grösste gemeinschaftliche Divisor von r und $\delta = \varepsilon\delta'$, so muss h durch δ' theilbar sein; die kleinste Zahl h, welche diese Bedingung erfüllt, ist offenbar δ' selbst, und dann ist auch wirklich

$$(a^r)^h = (a^\delta)^{\frac{r}{\varepsilon}} \equiv 1 \text{ (mod. } p);$$

also ist δ' die Zahl, zu welcher a^r gehört. Soll also a^r zum Exponenten δ gehören, so muss $\varepsilon = 1$, also r relative Primzahl gegen δ sein; und umgekehrt, sobald dies der Fall, also $\varepsilon = 1$ ist, gehört auch a^r wirklich zum Exponenten δ. Wir erhalten so das Resultat, dass unter den Zahlen (A) genau ebenso viele zu dem Exponenten δ gehören, als es unter den Exponenten

$$0,\ 1,\ 2 \ldots (\delta - 1)$$

relative Primzahlen zu δ giebt; es giebt daher $\varphi(\delta)$ solche Zahlen.

Da wir angenommen hatten, dass *mindestens eine* solche Zahl a existirte, so können wir das Bisherige so zusammenfassen: Ist p eine Primzahl und δ ein Divisor von $p-1$, so ist die Anzahl

der incongruenten Zahlen, die zu δ gehören, entweder $= 0$, oder $= \varphi(\delta)$. Um nun über diese Alternative zu entscheiden, betrachten wir die Totalität aller $p-1$ nach dem Modul p incongruenten und durch p nicht theilbaren Zahlen; wir theilen dieselben in Gruppen ein, indem wir je zwei incongruente Zahlen in dieselbe oder in verschiedene Gruppen werfen, je nachdem sie zu demselben Divisor δ von $p-1$ gehören oder zu verschiedenen. Bezeichnen wir mit $\psi(\delta)$ die Anzahl der Individuen, welche in die dem Divisor δ entsprechende Gruppe gehören, so muss, da jede der $p-1$ vertheilten Zahlen in eine, aber auch nur in eine solche Gruppe gehört,

$$\Sigma\, \psi(\delta) = p-1$$

sein, wo sich das Summenzeichen auf sämmtliche Divisoren δ von $p-1$ bezieht; wir wissen ferner schon, dass

$$\psi(\delta) \text{ entweder } = 0, \quad \text{oder } = \varphi(\delta)$$

ist. Da nun früher bewiesen ist (§. 13), dass auch

$$\Sigma\, \varphi(\delta) = p-1$$

ist, so folgt hieraus mit Nothwendigkeit, dass

$$\psi(\delta) \text{ niemals } = 0, \text{ sondern stets } = \varphi(\delta)$$

ist. Denn da jedes Glied $\psi(\delta)$ der erstern Summe dem entsprechenden der letztern höchstens gleich sein, aber niemals dasselbe übertreffen kann, so würde, sobald nur ein einziges Mal oder öfter $\psi(\delta) = 0$ wäre, die erstere Summe nothwendig kleiner ausfallen müssen als die letztere, während sie in der That einander gleich sind. Wir haben so den wichtigen Satz*) gewonnen:

Die Anzahl der sämmtlichen incongruenten Zahlen, welche zu einem bestimmten Divisor δ von $p-1$ gehören ist stets $= \varphi(\delta)$.

Es genügt, einen Blick auf das obige Beispiel zu werfen, in welchem $p = 7$, um diesen Satz bestätigt zu sehen.

§. 30.

Am interessantesten und folgenreichsten ist der in diesem Resultat enthaltene specielle Fall, in welchem $\delta = p-1$ ist:

Es giebt stets $\varphi(p-1)$ incongruente Zahlen g, welche zu dem Exponenten $p-1$ gehören, welche also die charakteristische Eigenschaft haben, dass die $p-1$ Potenzen

*) *Gauss: D. A.* art. 54.

$$1, g, g^2, g^3 \ldots g^{p-2} \qquad (G)$$

sämmtlich incongruent (mod. p) sind.

Da es überhaupt nur $p-1$ incongruente und durch p nicht theilbare Zahlen c giebt, so folgt, dass jede solche Zahl c einer, und natürlich auch nur einer der Potenzen (G) congruent ist. Jede solche Zahl g, welche zum Exponenten $p-1$ gehört, heisst eine *primitive Wurzel der Primzahl p**), und man kann daher sagen: wenn g eine primitive Wurzel von p ist, und c irgend eine durch p nicht theilbare Zahl, so existirt stets eine Zahl γ in der Reihe $0, 1, 2 \ldots p-2$ und nur eine von der Beschaffenheit, dass

$$c \equiv g^{\gamma} \text{ (mod. } p)$$

ist. Wenn man in dieser Weise alle incongruenten und — was im Folgenden immer hinzuzudenken ist — durch p nicht theilbaren Zahlen als Potenzen einer Basis g darstellt, so heissen die Exponenten γ die *Indices* der zugehörigen Zahlen c in Bezug auf die *Basis g*, und man schreibt z. B.

$$\text{Ind. } c = \gamma,$$

indem man die Basis g, so lange sie unverändert bleibt, in der Bezeichnung unterdrückt.

Nehmen wir z. B. $p = 13$, so überzeugt man sich leicht, dass 2 eine primitive Wurzel ist; denn durch Potenziren erhält man

$$2^0 \equiv 1,\quad 2^1 \equiv 2,\quad 2^2 \equiv 4,\quad 2^3 \equiv 8,\quad 2^4 \equiv 3,\quad 2^5 \equiv 6,$$
$$2^6 \equiv 12,\ 2^7 \equiv 11,\ 2^8 \equiv 9,\quad 2^9 \equiv 5,\quad 2^{10} \equiv 10,\ 2^{11} \equiv 7.$$

Nehmen wir daher 2 zur Basis eines Systems von Indices, so erhalten wir folgende Tabellen

c	1	2	3	4	5	6	7	8	9	10	11	12
Ind. c	0	1	4	2	9	5	11	3	8	10	7	6

und

Ind. c	0	1	2	3	4	5	6	7	8	9	10	11
c	1	2	4	8	3	6	12	11	9	5	10	7

deren erstere dazu dient, zu einer Zahl c den Index zu finden, während die zweite den entgegengesetzten Zweck hat**).

Offenbar hat dieses ganze Verfahren die grösste Analogie mit

*) *Euler*: *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, Nov. Comm. Petrop. XVIII, p. 85.

**) Im *Canon Arithmeticus* von *Jacobi* (1839) findet man solche Tabellen für alle dem ersten Tausend angehörenden Primzahlen.

der Construction von Logarithmentafeln, die ja auf dem ähnlichen Gedanken beruhen, alle positiven Zahlen als Potenzen einer einzigen Basis darzustellen; und es zeigt sich nun auch, dass in der Zahlentheorie die Indices ähnliche Gesetze befolgen und für praktische Zwecke ebenso brauchbar sind, wie die Logarithmen. Zunächst leuchtet ein, dass zwei congruente Zahlen auch stets denselben Index haben, in Zeichen: wenn $a \equiv b \pmod{p}$, so ist auch Ind. a = Ind. b. Ist ferner $c \equiv ab \pmod{p}$, so ist Ind. $c \equiv$ Ind. a + Ind. b (mod. $p-1$), oder kürzer, es ist stets

$$\text{Ind.}\,(ab) \equiv \text{Ind.}\,a + \text{Ind.}\,b \pmod{p-1}.$$

Denn es ist ja

$$a \equiv g^{\text{Ind.}a} \pmod{p}; \quad b \equiv g^{\text{Ind.}b} \pmod{p},$$

also

$$ab \equiv g^{\text{Ind.}a+\text{Ind.}b} \pmod{p};$$

nun ist aber auch

$$ab \equiv g^{\text{Ind.}(ab)} \pmod{p},$$

folglich

$$g^{\text{Ind.}(ab)} \equiv g^{\text{Ind.}a+\text{Ind.}b} \pmod{p}.$$

Da nun g eine primitive Wurzel von p, also eine zum Exponenten $\delta = (p-1)$ gehörende Zahl ist, so folgt aus §. 28 die Richtigkeit der zu beweisenden Congruenz nach dem Modul $p-1$. Nehmen wir unser obiges Beispiel, in welchem $p = 13$, so ist z. B.

$$\text{Ind.}\,(7) = 11, \quad \text{Ind.}\,(9) = 8,$$

folglich

$$\text{Ind.}\,(63) \equiv 19 \pmod{12}$$

oder

$$\text{Ind.}\,(63) = 7.$$

In der That ist aber $63 \equiv 11 \pmod{13}$, und Ind. (11) = 7. Man sieht aus diesem Beispiel, wie eine solche Doppeltafel der Indices dazu benutzt werden kann, mit Leichtigkeit die Classe (11) zu finden, welcher das Product (63) aus zwei Zahlen (7 und 9) angehört.

Natürlich lässt sich der vorstehende Satz auf ein Product aus beliebig vielen Factoren in folgender Weise ausdehnen:

$$\text{Ind.}\,(abc\ldots) \equiv \text{Ind.}\,a + \text{Ind.}\,b + \text{Ind.}\,c + \cdots \pmod{p-1}.$$

Nimmt man hierin alle Factoren einander congruent, so erhält man:

$$\text{Ind.}\,(a^n) \equiv n\ \text{Ind.}\,a \pmod{p-1},$$

wo n irgend eine positive ganze Zahl bedeutet.

Es liesse sich hieraus auch leicht nachweisen, dass der Uebergang von einem System von Indices zu einem andern, dessen Basis eine andere der $\varphi(p-1)$ primitiven Wurzeln ist, ganz ähnlichen Gesetzen unterliegt, wie der Uebergang von einem Logarithmensystem zu einem andern; wir beschränken uns indessen auf folgende einfache Bemerkungen. Wie auch die Basis g gewählt sein mag, der Index von 1 ist stets $= 0$; denn es ist immer $g^0 = 1$. Ferner ist (den Fall $p = 2$ ausgenommen) der Index von -1 stets $= \frac{1}{2}(p-1)$; denn da nach §. 19

$$g^{p-1} - 1 = (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

ist, so muss mindestens eine der beiden Zahlen

$$g^{\frac{p-1}{2}} - 1, \quad g^{\frac{p-1}{2}} + 1$$

durch p theilbar sein; die erstere ist es aber nicht, denn sonst wäre

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

was mit der Voraussetzung im Widerspruch ist, dass g zum Exponenten $p-1$ gehört; es ist daher stets

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

und folglich

$$\text{Ind.}\,(-1) = \frac{p-1}{2}.$$

Es verdient endlich noch bemerkt zu werden, dass man die Indices, statt aus den Zahlen $0, 1, 2 \ldots (p-2)$, ebenso gut aus jedem andern vollständigen System incongruenter Zahlen in Bezug auf den Modul $p-1$ wählen kann; die so eben bewiesenen Fundamentalsätze erleiden dadurch nicht die geringste Aenderung.

Man kann nun die Indices benutzen, um eine Congruenz ersten Grades

$$ax \equiv b \pmod{p},$$

die hier die Stelle eines Divisionsproblems vertritt, mit Leichtigkeit aufzulösen; denn es muss offenbar

$$\text{Ind.}\,x \equiv \text{Ind.}\,b - \text{Ind.}\,a \pmod{p-1}$$

sein. Ist also z. B. die Congruenz

$$5x \equiv 6 \pmod{13}$$

zu lösen, so wird man, indem man wieder die primitive Wurzel 2 zur Basis des Indexsystems wählt,

$$\text{Ind. } x \equiv \text{Ind. } 6 - \text{Ind. } 5 \equiv 5 - 9 \equiv 8 \pmod{12}$$

und folglich

$$x \equiv 9 \pmod{13}$$

finden.

Diese Methode, Congruenzen ersten Grades aufzulösen, scheint auf den ersten Blick nur dann anwendbar, wenn der Modul eine Primzahl ist; allein man kann leicht zeigen, dass jede beliebige Congruenz ersten Grades

$$ax \equiv b \pmod{k},$$

deren Modul eine zusammengesetzte Zahl ist, auf eine Kette von Congruenzen reducirt werden kann, deren Moduln Primzahlen sind. Wir können uns hierbei auf den Fall beschränken, in welchem a relative Primzahl gegen k ist. Man löse nun zuerst die Congruenz

$$ax \equiv b \pmod{p},$$

wo p irgend eine in $k = pk'$ aufgehende Primzahl ist, nach der neuen Methode, so erhält man ein Resultat von der Form

$$x \equiv \alpha \pmod{p} \quad \text{oder} \quad x = \alpha + px',$$

wo x' eine beliebige ganze Zahl ist; substituirt man diesen Ausdruck in die gegebene Congruenz, so nimmt sie die folgende Form an:

$$pax' \equiv b - a\alpha \pmod{k}.$$

Da nun $b - a\alpha$ durch p theilbar, also von der Form $b'p$ ist, so stimmen sämmtliche Wurzeln der vorstehenden Congruenz mit den sämmtlichen Wurzeln der Congruenz

$$ax' \equiv b' \pmod{k'}$$

überein. Auf dieselbe Weise kann man nun fortfahren, indem man diese Congruenz zunächst nur in Bezug auf eine in k' aufgehende Primzahl p' löst, u. s. f.; man braucht dann zuletzt nur noch von der Wurzel der letzten dieser Congruenzen durch successive Substitution zu der der ursprünglichen überzugehen.

§. 31.

Wir benutzen nun noch die Theorie der Indices, um auf sie die Theorie der *binomischen Congruenzen* für einen Primzahl-

modulus p zu stützen; nach einer frühern Bemerkung kann man einer jeden solchen binomischen Congruenz die Form

$$x^n \equiv D \pmod{p} \qquad (1)$$

geben, in welcher der Coefficient der Potenz der Unbekannten $= 1$ ist; da ferner der Fall, in welchem $D \equiv 0 \pmod{p}$ und folglich auch $x \equiv 0 \pmod{p}$, ohne Interesse ist, so schliessen wir denselben aus.

Bezeichnen wir nun zur Abkürzung die Indices von D und x resp. mit γ und ξ (wenn irgend eine primitive Wurzel g von p zur Basis genommen ist), so reducirt sich die Auflösung der Congruenz (1) auf die Bestimmung aller Wurzeln ξ der Congruenz ersten Grades

$$n\xi \equiv \gamma \pmod{p-1}; \qquad (2)$$

denn offenbar entspricht jeder Wurzel der einen dieser beiden Congruenzen (1) und (2) auch stets eine und nur eine Wurzel der andern.

Es sei jetzt δ der grösste gemeinschaftliche Divisor der Zahlen $p-1$ und n, so ist (§. 22) die Congruenz (2) nur dann möglich, wenn die Bedingung

$$\gamma \equiv 0 \pmod{\delta} \qquad (3)$$

erfüllt ist, und dann hat sie δ nach dem Modul $p-1$ incongruente Wurzeln ξ. Wir schliessen hieraus unmittelbar den Satz:

Ist δ der grösste gemeinschaftliche Divisor des Grades n der Congruenz (1) *und der Zahl $p-1$, so ist diese Congruenz nur dann möglich, wenn die Bedingung*

$$\text{Ind. } D \equiv 0 \pmod{\delta} \qquad (4)$$

erfüllt ist, und dann besitzt sie δ nach dem Modul p incongruente Wurzeln x.

Liegt z. B. die Congruenz

$$x^8 \equiv 3 \pmod{13}$$

vor, so ist $\delta = 4$; nehmen wir ferner die primitive Wurzel 2 als Basis für die Indices, so ist Ind. $3 = 4$, also ist die Bedingung (4) erfüllt, und die vorgelegte Congruenz hat 4 nach dem Modul 13 incongruente Wurzeln; um diese zu finden, bilden wir die Congruenz ersten Grades

$$8\xi \equiv 4 \pmod{12} \quad \text{oder} \quad 2\xi \equiv 1 \pmod{3},$$

und erhalten hieraus

$$\xi \equiv 2 \pmod{3}$$

oder

$$\xi \equiv 2, \text{ oder } 5, \text{ oder } 8, \text{ oder } 11 \pmod{12},$$

folglich, indem wir zu diesen Indices ξ die zugehörigen Zahlen suchen,

$$x \equiv 4, \text{ oder } 6, \text{ oder } 9, \text{ oder } 7 \pmod{13}.$$

Da die Möglichkeit der binomischen Congruenz von der Wahl der primitiven Wurzel g, auf welche sich die Indices γ und ξ beziehen, nothwendig unabhängig sein muss, so wird das Kriterium, dass der Index γ einer Zahl D durch einen Divisor δ der Zahl $p-1$ theilbar sein muss, in eine von der Theorie der Indices unabhängige Form gebracht werden können. Dies bestätigt sich auf folgende Weise. Sobald in Bezug auf irgend eine Basis g der Index γ der Zahl D durch den Divisor δ von $p-1$ theilbar, also von der Form $h\delta$ ist, so haben wir die Congruenz

$$D \equiv g^{h\delta} \pmod{p}$$

und hieraus durch Potenzirung

$$D^{\frac{p-1}{\delta}} \equiv g^{h(p-1)} \equiv 1 \pmod{p};$$

und umgekehrt, sobald die Zahl D dieser Bedingung

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$$

genügt, muss der in Bezug auf eine beliebige Basis g genommene Index γ der Zahl D durch δ theilbar sein; denn es sei

$$D \equiv g^{\gamma} \pmod{p},$$

so folgt hieraus

$$g^{\gamma \cdot \frac{p-1}{\delta}} \equiv 1 \pmod{p},$$

und da g eine primitive Wurzel, d. h. eine zum Exponenten $p-1$ gehörende Zahl ist, so muss der Exponent durch $p-1$, und folglich der Index γ durch δ theilbar sein.

Nachdem das ursprüngliche Kriterium so umgeformt ist, können wir unsern Satz in folgender Weise unabhängig von der Theorie der Indices aussprechen:

Ist δ der grösste gemeinschaftliche Divisor der Zahlen n und $p-1$, so hat die Congruenz

$$x^n \equiv D \pmod{p}, \qquad (1)$$

genau δ incongruente Wurzeln, oder gar keine, je nachdem die Zahl D der Bedingung

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p} \qquad (5)$$

genügt oder nicht genügt.

Den speciellen Fall, in welchem $\delta = n$ und $D = 1$ ist, haben wir schon früher (§. 27) auf anderm Wege bewiesen; es würde nicht schwer sein, aus den dort angewandten Principien auch den allgemeinen Satz abzuleiten, ohne die Theorie der Indices zu Hülfe zu rufen; doch überlassen wir der Kürze halber diese Untersuchung dem Leser.

Wir können nun auch noch die Frage aufstellen: wenn der Grad n der Congruenz (1) gegeben ist, wie viele incongruente Zahlen D existiren, für welche die Congruenz (1) möglich ist? Hierauf liefert der Satz selbst sogleich die Antwort, denn diese Zahlen D sind ja die sämmtlichen Wurzeln der binomischen Congruenz

$$x^{\frac{p-1}{\delta}} \equiv 1 \pmod{p};$$

der grösste gemeinschaftliche Divisor des Exponenten $(p-1):\delta$ und der Zahl $p-1$ ist in diesem Falle der Exponent $(p-1):\delta$ selbst, und da das Kriterium für die Möglichkeit offenbar erfüllt ist, so ist also die Anzahl aller incongruenten Zahlen D, für welche die Congruenz (1) möglich ist, genau $= (p-1):\delta$. Man nennt solche Zahlen D, welche einer $n$ten Potenz einer Zahl congruent sind, kurz $n$te Potenzreste, und wir können daher sagen:

Die Anzahl aller nten Potenzreste ist $= (p-1) : \delta$, *wo* δ *den grössten gemeinschaftlichen Divisor der Zahlen* n *und* $p-1$ *bezeichnet.*

Man findet dieselben offenbar, wenn man alle incongruenten Zahlen zur $n$ten Potenz erhebt und deren Reste bildet. Wenn $n = 2, 3, 4$ ist, so nennt man diese Zahlen resp. *quadratische, cubische, biquadratische Reste.* Mit der Theorie der erstern, welche für sich allein schon eine grosse Ausdehnung besitzt, werden wir uns nun im Folgenden ausführlich beschäftigen.

Dritter Abschnitt.

Von den quadratischen Resten.

§. 32.

Wir behandeln im Folgenden ausführlich die Theorie der Congruenzen von der Form

$$x^2 \equiv D \text{ (mod. } k), \qquad (1)$$

in welcher wir stets D als *relative Primzahl* gegen den Modul k voraussetzen. Es würde sich leicht zeigen lassen, dass jede beliebige Congruenz zweiten Grades auf diesen Fall zurückgeführt werden kann; doch wollen wir uns dabei nicht aufhalten. So oft nun die Congruenz (1) möglich ist, d. h. so oft sie Wurzeln hat, heisst die Zahl D *quadratischer Rest der Zahl* k; im entgegengesetzten Fall heisst D *quadratischer Nichtrest der Zahl* k. Man lässt auch häufig, wenn kein Missverständniss zu befürchten ist, das Beiwort „quadratisch“ fort und nennt kurz die Zahl D *Rest* oder *Nichtrest* von k, je nachdem die Congruenz (1) möglich ist oder nicht. Unmittelbar leuchtet hieraus ein, dass zwei nach dem Modul k congruente Zahlen entweder beide Reste von k, oder beide Nichtreste von k sind; d. h. alle in einer und derselben *Classe* enthaltenen Zahlen haben denselben Charakter; je nachdem eine von ihnen Rest oder Nichtrest des Modul k ist, sind sie alle Reste oder alle Nichtreste von k.

Die Theorie der quadratischen Reste zerfällt nun in zwei Haupttheile; man kann nämlich einmal die Frage aufwerfen:

Wenn der Modul k gegeben ist, welches sind dann die sämmtlichen incongruenten quadratischen Reste von k? und wie viele Wurzeln hat die einer jeden dieser Zahlen entsprechende Congruenz?

Bei weitem schwieriger ist aber die Beantwortung der folgenden zweiten Hauptfrage:

Wenn die Zahl D gegeben ist, welches sind dann die Moduln k, für welche die Congruenz (1) möglich ist, d. h. welches sind die Zahlen k, von denen die gegebene Zahl D quadratischer Rest ist?

§. 33.

Wir beschäftigen uns zuerst mit der ersten Frage und beginnen die Untersuchung mit dem einfachsten Falle, mit dem nämlich, wo der Modul eine *ungerade Primzahl* p ist (der Fall $p = 2$ erledigt sich unmittelbar durch die Bemerkung, dass jede ungerade Zahl $\equiv 1^2$, also quadratischer Rest von 2 ist). Hier erhalten wir die vollständige Antwort sogleich durch die vorhergehende Theorie der binomischen Congruenzen (§. 31). In unserm Falle ist nämlich $n = 2$ der Grad der binomischen Congruenz, und da $p - 1$ gerade ist, so ist $\delta = 2$ der grösste gemeinschaftliche Divisor von n und $p - 1$; die Congruenz

$$x^2 \equiv D \pmod{p}$$

ist daher stets und nur dann möglich, wenn

$$D^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

und zwar hat sie jedesmal zwei incongruente Wurzeln; es giebt $\frac{1}{2}(p-1)$ quadratische Reste, und folglich, da die Anzahl aller incongruenten und durch p nicht theilbaren Zahlen gleich $p - 1$ ist, auch $\frac{1}{2}(p-1)$ Nichtreste von p. Da ferner nach dem Fermat'schen Satze

$$D^{p-1} - 1 = (D^{\frac{p-1}{2}} - 1)(D^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

ist, so folgt, dass

$$D^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

sein muss, so oft D ein Nichtrest von p ist. Je nachdem also

$D^{\frac{p-1}{2}} \equiv +1$ oder $\equiv -1$ ist, ist D ein Rest oder Nichtrest von p. Nennt man die Eigenschaft einer Zahl D, Rest oder Nichtrest von p zu sein, ihren *Charakter*, so ist derselbe also durch dieses Kriterium vollständig bestimmt*).

Es lässt sich indessen auch ganz elementar beweisen, dass die Anzahl sowohl der Reste als auch der Nichtreste $= \frac{1}{2}(p-1)$ ist. Quadrirt man nämlich die $\frac{1}{2}(p-1)$ Zahlen

$$1,\ 2,\ 3, \ldots \frac{p-1}{2},$$

so sind die Quadrate sämmtlich incongruent; denn sind r und s zwei verschiedene dieser Zahlen, so ist die Differenz ihrer Quadrate

$$r^2 - s^2 = (r+s)(r-s)$$

nicht theilbar durch p, da die Factoren $r+s$ und $r-s$ kleiner als p sind. Diese $\frac{1}{2}(p-1)$ Quadrate geben also wirklich $\frac{1}{2}(p-1)$ incongruente quadratische Reste; dagegen liefern die Quadrate der folgenden Zahlen

$$\frac{p+1}{2},\ \frac{p+3}{2} \cdots (p-1)$$

dieselben Reste wieder; denn es ist allgemein

$$(p-r)^2 = p^2 - 2rp + r^2 \equiv r^2 \pmod{p}.$$

Also ist $\frac{1}{2}(p-1)$ die Anzahl aller quadratischen Reste, und folglich auch die der quadratischen Nichtreste.

Da ein Product aus mehreren Factoren, die nicht durch p theilbar sind, dieselbe Eigenschaft hat, so kann man nach dem Charakter des Productes fragen, wenn die Charaktere der Factoren gegeben sind. Beschränken wir uns zunächst auf zwei Factoren, so sind folgende drei Fälle zu unterscheiden.

I. Das Product aus zwei Resten ist wieder ein Rest; denn sind a und a' Reste, so giebt es Zahlen x, x' von der Beschaffenheit, dass $a \equiv x^2 \pmod{p}$, $a' \equiv x'^2 \pmod{p}$; hieraus folgt aber $aa' \equiv (xx')^2 \pmod{p}$, d. h. aa' ist Rest von p.

II. Das Product aus einem Rest und einem Nichtrest ist ein Nichtrest. Denn wenn wir ein vollständiges System incongruenter

*) Dies Kriterium rührt wesentlich von *Euler* her; man vergl. z. B. die Abhandlung *Theoremata circa residua ex divisione potestatum relicta*, Nov. Comm. Petrop. VII, p. 49; aber es ist mir nicht geglückt, in seinen zahlreichen Arbeiten über diesen Gegenstand eine Stelle aufzufinden, wo dasselbe in voller Schärfe ausgesprochen wäre.

und durch p nicht theilbarer Zahlen bilden, so zerfällt dasselbe in zwei Gruppen, deren eine $\frac{1}{2}(p-1)$ Reste — wir wollen sie allgemein mit α bezeichnen — und deren zweite $\frac{1}{2}(p-1)$ Nichtreste β enthält. Multiplicirt man nun alle diese Zahlen α und β mit einem Reste a, so bilden die Producte $a\alpha$ und $a\beta$ wieder ein vollständiges System incongruenter (durch p nicht theilbarer) Zahlen, welches also wieder $\frac{1}{2}(p-1)$ Reste und $\frac{1}{2}(p-1)$ Nichtreste enthält. In der That sind nun (nach I.) die Producte $a\alpha$ sämmtlich wieder Reste; es müssen daher die anderen $\frac{1}{2}(p-1)$ Producte $a\beta$ sämmtlich Nichtreste sein; also ist das Product aus jedem Rest a und jedem Nichtrest β ein Nichtrest.

III. Das Product aus zwei Nichtresten ist ein Rest. Denn bildet man wieder das System der Reste α und Nichtreste β, und multiplicirt dieselben mit einem Nichtreste b, so sind die Producte $b\alpha$ (nach II.) sämmtlich Nichtreste; folglich müssen die übrigen $\frac{1}{2}(p-1)$ Producte $b\beta$ sämmtlich Reste sein.

Man kann diese wichtigen Sätze offenbar in den folgenden einen zusammenfassen:

Ein Product aus beliebig vielen durch die Primzahl p nicht theilbaren Zahlen ist Rest oder Nichtrest von p, je nachdem die Anzahl der Nichtreste, welche sich unter den Factoren finden, gerade oder ungerade ist.

Dieser Satz ergiebt sich auch unmittelbar aus dem oben aufgestellten Kriterium für den Charakter einer Zahl; denn da

$$(abc\ldots)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\, b^{\frac{p-1}{2}}\, c^{\frac{p-1}{2}} \ldots$$

ist, so wird

$$(abc\ldots)^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}$$

sein, je nachdem die Anzahl der Factoren $a^{\frac{p-1}{2}}, b^{\frac{p-1}{2}}, c^{\frac{p-1}{2}}, \ldots$, welche $\equiv -1$ sind, eine gerade oder ungerade ist.

Man kann diesen Satz in Form einer Gleichung ausdrücken, wenn man sich eines von *Legendre**) in die Zahlentheorie eingeführten Zeichens bedient, welches in allen folgenden Untersuchungen eine grosse Rolle spielt. *Legendre* bezeichnet nämlich durch das Symbol

$$\left(\frac{m}{p}\right)$$

*) *Théorie des Nombres*, 3me éd. Tom. I. p. 197.

die positive oder negative Einheit, je nachdem die durch die Primzahl p nicht theilbare Zahl m quadratischer Rest oder Nichtrest von p ist; es ist daher stets

$$\left(\frac{m}{p}\right)\left(\frac{m}{p}\right) = +1 \quad \text{und} \quad m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \pmod{p}.$$

Den Satz über den Charakter eines Productes kann man dann offenbar durch die folgende Gleichung ausdrücken:

$$\left(\frac{mnl\ldots}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\left(\frac{l}{p}\right)\cdots$$

Es leuchtet ferner ein, dass, sobald $m \equiv n \pmod{p}$, auch

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$$

sein wird.

§. 34.

Es ist nun interessant zu sehen, dass die soeben gewonnenen Sätze, welche zum Theil als Resultate einer ausgedehnten Theorie, wie der der binomischen Congruenzen, erscheinen, sich aus den ersten Principien auf einem ganz elementaren Wege ableiten lassen, der zugleich einen neuen Beweis des Wilson'schen und Fermat'schen Satzes liefern wird.

Es sei D irgend eine durch die (ungerade) Primzahl p nicht theilbare Zahl, und r irgend eine der Zahlen

$$1, 2, 3 \ldots (p-1); \tag{1}$$

dann existirt in derselben Reihe stets eine und nur eine Zahl s von der Beschaffenheit, dass

$$rs \equiv D \pmod{p}$$

ist; denn diese Zahl s ist ja die Wurzel der Congruenz ersten Grades $rx \equiv D \pmod{p}$; je zwei solche Zahlen r und s der Reihe (1), deren Product $\equiv D$ ist, wollen wir *zusammengehörige* Zahlen nennen; offenbar ist durch eine dieser beiden Zahlen die andere ebenfalls bestimmt. Identisch können diese beiden Zahlen nur dann werden, wenn die Congruenz

$$x^2 \equiv D \pmod{p} \tag{2}$$

möglich ist. Danach theilen wir unsere Untersuchung in zwei Fälle ein.

Erstens: Die Congruenz (2) ist unmöglich. — Dann sind also je zwei zusammengehörige Zahlen von einander verschieden, und da zwei solche Paare stets identisch sind, sobald sie nur eine gemeinschaftliche Zahl haben, so zerfallen die sämmtlichen $p-1$ Zahlen (1) in $\frac{1}{2}(p-1)$ solche Paare zusammengehöriger Zahlen, und folglich ist ihr Product

$$1 \,.\, 2 \,.\, 3 \ldots (p-1) \equiv D^{\frac{p-1}{2}} \pmod{p}. \qquad (3)$$

Zweitens: Die Congruenz (2) ist möglich. — Dann existirt also auch in der Reihe (1) mindestens eine Zahl ϱ von der Beschaffenheit, dass $\varrho^2 \equiv D$; sehen wir zu, ob ausser ϱ in der Reihe (1) noch eine solche Zahl σ existirt; dann muss $\sigma^2 \equiv \varrho^2$, folglich $(\sigma-\varrho)(\sigma+\varrho)$ durch p theilbar sein; da wir σ verschieden von ϱ voraussetzen, so ist $\sigma-\varrho$ nicht theilbar durch p, folglich muss $\sigma+\varrho$ theilbar durch p, also $\sigma = p-\varrho$ sein; und in der That ist wirklich $(p-\varrho)^2 \equiv D$. Trennen wir nun diese beiden (wirklich ungleichen) Zahlen ϱ und $\sigma = p-\varrho$, deren Product $\varrho\sigma \equiv -\varrho^2 \equiv -D$ ist, von den übrigen der Reihe (1), so zerfallen die letztern in $\frac{1}{2}(p-3)$ Paare zusammengehöriger Zahlen von der Beschaffenheit, dass jedes Paar aus zwei verschiedenen Zahlen besteht. Demnach ist in diesem Fall das Product aller Zahlen der Reihe (1):

$$1 \,.\, 2 \,.\, 3 \ldots (p-1) \equiv -D^{\frac{p-1}{2}} \pmod{p}. \qquad (4)$$

Nun giebt es aber einen Fall, in welchem die Congruenz (2) stets möglich ist, nämlich den, in welchem $D = 1 = 1^2$; wir erhalten daher zunächst aus (4) den Satz von *Wilson:*

$$1 \,.\, 2 \,.\, 3 \ldots (p-1) \equiv -1 \pmod{p}, \qquad (5)$$

und substituiren wir dies in die Congruenzen (3) und (4), so erhalten wir das Resultat, dass

$$D^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}$$

ist, je nachdem die Congruenz (2) möglich oder nicht möglich ist. Da endlich ein dritter Fall nicht existiren kann, so erhalten wir allgemein

$$D^{p-1} = (D^{\frac{p-1}{2}})^2 \equiv (\pm 1)^2 \equiv +1 \pmod{p},$$

also den Satz von *Fermat.*

Durch diese einfache Betrachtung sind wir also sogleich bis zu denselben Sätzen in der Theorie der quadratischen Reste ge-

langt, welche vorher aus der allgemeinen Theorie der binomischen Congruenzen abgeleitet waren.

§. 35.

Wir wenden uns jetzt zu der Untersuchung des Falls, in welchem der Modul k der quadratischen Congruenz

$$x^2 \equiv D \pmod{k}$$

die Potenz einer Primzahl p ist; dabei müssen wir den Fall, in welchem $p = 2$, gesondert von den übrigen behandeln, in welchen p eine ungerade Primzahl ist*).

Ist zunächst p eine ungerade Primzahl, und $k = p^\pi$, wo π irgend eine positive ganze Zahl bedeutet, und nehmen wir an, die Congruenz

$$x^2 \equiv D \pmod{p^\pi} \tag{1}$$

sei möglich, so überzeugt man sich leicht, dass sie im Ganzen *zwei* incongruente Wurzeln hat; denn ist α eine bestimmte, und x irgend eine Wurzel, so muss

$$x^2 - \alpha^2 = (x - \alpha)(x + \alpha) \equiv 0 \pmod{p^\pi}$$

sein; von den beiden Factoren $x - \alpha$ und $x + \alpha$ ist aber nur einer durch p theilbar; denn wären beide durch p theilbar, so wäre auch ihre Differenz 2α, und folglich auch α durch p theilbar, was nicht der Fall ist, da wir $D \equiv \alpha^2$ als nicht theilbar durch p vorausgesetzt haben. Da also einer der beiden Factoren relative Primzahl gegen p^π ist, so muss der andere für sich allein durch p^π theilbar sein. Es ist daher entweder

$$x \equiv \alpha \pmod{p^\pi}, \quad \text{oder} \quad x \equiv -\alpha \pmod{p^\pi};$$

also hat die Congruenz (1) entweder gar keine Wurzel, oder sie hat zwei incongruente Wurzeln α und $-\alpha$.

Es ist nun noch zu entscheiden, wann das Eine, wann das Andere Statt finden wird. Da nun jede Wurzel α der Congruenz (1) auch eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p} \tag{2}$$

ist, so leuchtet ein, dass die Congruenz (1) nur dann möglich ist, wenn D quadratischer Rest von p ist; es fragt sich daher nur, ob

*) Die nachfolgenden Resultate lassen sich auch aus dem in §. 145 bewiesenen Satze ableiten.

auch umgekehrt, wenn D quadratischer Rest von p ist, hieraus die Möglichkeit der Congruenz (1) folgt. Um dies zu zeigen, brauchen wir nur nachzuweisen, dass, sobald die Congruenz (2) eine Wurzel α besitzt (also D quadratischer Rest von p ist), hieraus sich eine Wurzel der Congruenz (1) ableiten lässt, welche $\equiv \alpha \pmod{p}$ ist; und da Aehnliches von jeder Congruenz $x^2 \equiv D \pmod{k}$ gilt, wo D stets dieselbe Zahl, k aber irgend eine Potenz der Primzahl p ist, so braucht man nur zu zeigen, dass aus einer Wurzel α der Congruenz (1) sich eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p^{\pi+1}} \tag{3}$$

ableiten lässt, welche $\equiv \alpha \pmod{p^\pi}$ ist. Es sei daher

$$\alpha^2 \equiv D \pmod{p^\pi} \quad \text{oder} \quad \alpha^2 - D = hp^\pi,$$

so setzen wir

$$x = \alpha + p^\pi y,$$

woraus

$$x^2 - D = hp^\pi + 2\alpha p^\pi y + p^{2\pi} y^2 \equiv p^\pi (h + 2\alpha y) \pmod{p^{\pi+1}}$$

folgt; damit nun $x^2 \equiv D \pmod{p^{\pi+1}}$ werde, braucht y nur so bestimmt zu werden, dass

$$2\alpha y \equiv -h \pmod{p}$$

werde; da nun D, folglich auch α und also, da p ungerade ist, auch 2α eine durch p nicht theilbare Zahl ist, so lässt sich y stets so wählen, dass es dieser Congruenz ersten Grades genügt. Wir sehen also, dass aus der Möglichkeit der Congruenz (1) auch stets die Möglichkeit der Congruenz (3) folgt; durch dieselbe wiederholt angewendete Schlussweise ergiebt sich also auch, dass aus der Möglichkeit der Congruenz (2) stets die der Congruenz (1) folgt, und wir haben auch eine Methode gefunden, um aus einer Wurzel der Congruenz $x^2 \equiv D$ für den Modul p successive eine Wurzel derselben Congruenz für die Moduln p^2, $p^3 \ldots p^\pi$ zu gewinnen. Wir haben mithin folgendes Resultat:

Ist p eine ungerade Primzahl, und D eine durch p nicht theilbare Zahl, so ist für die Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{p^\pi}$$

erforderlich und hinreichend, dass

$$\left(\frac{D}{p}\right) = 1,$$

d. h. dass D quadratischer Rest von p sei; sobald diese Bedingung erfüllt ist, besitzt die vorgelegte Congruenz zwei incongruente Wur-

zeln α und $-\alpha$, welche gefunden werden können, sobald man eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p}$$

gefunden hat.

§. 36.

Wir gehen nun zu dem besondern Fall über, in welchem der Modul k eine Potenz der Primzahl 2 ist, so dass also D irgend eine ungerade Zahl bedeutet. Betrachten wir zunächst die Congruenz

$$x^2 \equiv D \pmod{4},$$

so erkennt man leicht, dass dieselbe stets und nur dann möglich ist, wenn

$$D \equiv 1 \pmod{4}$$

ist. Denn ist die Congruenz möglich, so ist x jedenfalls ungerade, und das Quadrat von $x = 2n + 1$ ist $4n^2 + 4n + 1 \equiv 1 \pmod{4}$; umgekehrt, ist $D \equiv 1 \pmod{4}$, so hat die Congruenz offenbar die beiden incongruenten Wurzeln $x \equiv 1$ und $x \equiv -1 \pmod{4}$.

Gehen wir nun zu der Congruenz

$$x^2 \equiv D \pmod{8}$$

über, so leuchtet ein, da das Quadrat einer jeden ungeraden Zahl $4n \pm 1$ gleich $16n^2 \pm 8n + 1 \equiv 1 \pmod{8}$ ist, dass diese Congruenz nur dann möglich ist, wenn

$$D \equiv 1 \pmod{8}$$

ist; und umgekehrt, sobald diese Bedingung erfüllt ist, hat die Congruenz die vier incongruenten Wurzeln $x \equiv 1$, $x \equiv 3$, $x \equiv 5$, $x \equiv 7$.

Betrachten wir jetzt die Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

wo $\pi \geqq 3$ ist, so kann diese Congruenz nur dann möglich sein, wenn die Congruenz

$$x^2 \equiv D \pmod{8}$$

möglich ist; es ist daher erforderlich, dass

$$D \equiv 1 \pmod{8}$$

sei. Wir wollen nun umgekehrt zeigen, dass diese Bedingung

auch hinreicht, und dass dann die Congruenz stets 4 incongruente Wurzeln hat. Nehmen wir nämlich an, dies sei für den Modul 2^π schon bewiesen, so können wir zeigen, dass dasselbe auch für den Modul $2^{\pi+1}$ gilt. Es sei nämlich α eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{2^\pi}$$

also

$$\alpha^2 - D = h \,.\, 2^\pi,$$

so setzen wir

$$x = \alpha + 2^{\pi-1} \,.\, y;$$

dann wird

$$x^2 - D = h \,.\, 2^\pi + 2^\pi \,.\, \alpha y + 2^{2\pi-2} y^2.$$

Da nun $\pi \geqq 3$, so ist $2\pi - 2 \geqq \pi + 1$, folglich

$$x^2 - D \equiv 2^\pi (h + \alpha y) \pmod{2^{\pi+1}}.$$

Damit also $x^2 - D$ durch $2^{\pi+1}$ theilbar werde, braucht man nur y so zu wählen, dass

$$\alpha y \equiv -h \pmod{2}$$

werde. Dies ist aber stets möglich, da α eine ungerade Zahl ist; also folgt aus der Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

wo $\pi \geqq 3$ ist, stets die Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{2^{\pi+1}}.$$

Wir schliessen hieraus zunächst das folgende Resultat:

Damit die Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

in welcher $\pi \geqq 3$ *ist, Wurzeln habe, ist erforderlich und hinreichend, dass*

$$D \equiv 1 \pmod{8}$$

sei.

Ist nun α eine Wurzel dieser Congruenz — und eine solche kann immer nach der obigen Methode gefunden werden —, so muss, wenn x irgend eine Wurzel derselben Congruenz bezeichnet,

$$x^2 - \alpha^2 = (x - \alpha)(x + \alpha) \equiv 0 \pmod{2^\pi}$$

sein. Da ferner α sowohl wie x ungerade Zahlen sein müssen, so sind die beiden Factoren $x - \alpha$ und $x + \alpha$ gerade Zahlen, und dann muss

$$\frac{x-\alpha}{2} \cdot \frac{x+\alpha}{2} \equiv 0 \pmod{2^{\pi-2}}$$

sein. Da nun die Differenz der beiden Factoren $\frac{1}{2}(x-\alpha)$ und $\frac{1}{2}(x+\alpha)$ eine ungerade Zahl ist, so muss einer von ihnen ungerade, und der andere folglich theilbar durch $2^{\pi-2}$ sein. Dies giebt folgende Fälle:

$$x \equiv \alpha \text{ (mod. } 2^{\pi-1}) \quad \text{oder} \quad x \equiv -\alpha \text{ (mod. } 2^{\pi-1})$$

und diese liefern wieder folgende vier Fälle:

$$x \equiv \alpha \text{ (mod. } 2^{\pi}); \qquad x \equiv \alpha + 2^{\pi-1} \text{ (mod. } 2^{\pi});$$
$$x \equiv -\alpha \text{ (mod. } 2^{\pi}); \quad x \equiv -(\alpha + 2^{\pi-1}) \text{ (mod. } 2^{\pi}).$$

Und umgekehrt überzeugt man sich leicht, dass jede dieser vier in Bezug auf den Modul 2^{π} incongruenten Zahlen der Congruenz genügt.

Wir fassen die ganze Untersuchung in folgendem Satze zusammen:

Die Congruenz

$$x^2 \equiv D \text{ (mod. } 2^{\pi})$$

ist stets möglich, wenn $\pi = 1$, *und hat dann eine Wurzel; sie ist, wenn* $\pi = 2$, *stets und nur dann möglich, wenn* $D \equiv 1$ (*mod.* 4) *und sie hat dann zwei Wurzeln; sie ist, wenn* $\pi \geqq 3$, *stets und nur dann möglich, wenn* $D \equiv 1$ (*mod.* 8) *ist, und zwar hat sie dann vier Wurzeln.*

§. 37.

Es ist jetzt leicht, die Möglichkeit und die Anzahl der Wurzeln der Congruenz $x^2 \equiv D$ für einen beliebigen Modulus zu beurtheilen, der relative Primzahl zu D ist. Wir führen diese Untersuchung ganz allgemein in folgender Weise.

Es seien a, b, c . . . relative Primzahlen zu einander, und

$$f(x) \equiv 0 \text{ (mod. } abc \ldots) \tag{1}$$

eine beliebige zur Auflösung vorgelegte Congruenz, so lässt dieselbe sich stets auf die vollständige Auflösung der Congruenzen

$$\left.\begin{array}{l} f(x) \equiv 0 \text{ (mod. } a) \\ f(x) \equiv 0 \text{ (mod. } b) \\ f(x) \equiv 0 \text{ (mod. } c) \end{array}\right\} \tag{2}$$

u. s. w.

zurückführen. Zunächst leuchtet ein, dass jede Wurzel x der Congruenz (1) auch allen Congruenzen (2) genügen muss; es wird daher die Congruenz (1) unmöglich sein, wenn dies mit irgend einer der Congruenzen (2) der Fall ist. Umgekehrt, ist α irgend eine Wurzel der Congruenz $f(x) \equiv 0$ (mod. a), ebenso β irgend eine Wurzel der Congruenz $f(x) \equiv 0$ (mod. b), γ eine Wurzel der Congruenz $f(x) \equiv 0$ (mod. c) u. s. w., so bestimme man (nach §. 25) eine Zahl x durch das System von Congruenzen

$$\left.\begin{array}{l} x \equiv \alpha \text{ (mod. } a) \\ x \equiv \beta \text{ (mod. } b) \\ x \equiv \gamma \text{ (mod. } c) \end{array}\right\} \quad (3)$$
u. s. w.,

so wird

$$f(x) \equiv f(\alpha) \equiv 0 \text{ (mod. } a)$$
$$f(x) \equiv f(\beta) \equiv 0 \text{ (mod. } b)$$
$$f(x) \equiv f(\gamma) \equiv 0 \text{ (mod. } c)$$
u. s. w.

und folglich, da $a, b, c \ldots$ relative Primzahlen zu einander sind, auch

$$f(x) \equiv 0 \text{ (mod. } abc \ldots),$$

d. h. jede dem System (3) genügende Zahl x ist eine Wurzel der vorgelegten Congruenz (1). Da nun (nach §. 25) dem System (3) unendlich viele Zahlen x genügen, welche aber alle nach dem Modul $abc \ldots$ einander congruent sind, so liefert das System (3) eine und nur eine Wurzel x der Congruenz (1). Ist nun

λ die Anzahl aller incongruenten Wurzeln α (mod. a)
μ " " " " " β (mod. b)
ν " " " " " γ (mod. c)
u. s. w.

so kann man im Ganzen $\lambda\mu\nu \ldots$ verschiedene Systeme (3) bilden, welchen (nach §. 25) ebensoviele verschiedene Wurzeln x der Congruenz (1) entsprechen; und andere Wurzeln kann diese letztere nicht besitzen, weil, wie schon oben bemerkt ist, jede bestimmte Wurzel x der Congruenz (1) auch Wurzel aller Congruenzen (2) und folglich einem bestimmten α (mod. a), einem bestimmten β (mod. b), einem bestimmten γ (mod. c) u. s. f. congruent sein muss. Mithin ist die Anzahl aller nach dem Modul $abc \ldots$ incongruenten Wurzeln der vorgelegten Congruenz $= \lambda\mu\nu \ldots$

Mit Hülfe dieses allgemeinen Resultates sind wir im Stande zu beurtheilen, ob die Congruenz

$$x^2 \equiv D \pmod{k},$$

in welcher D und k relative Primzahlen sind, möglich, und wie gross die Anzahl σ ihrer incongruenten Wurzeln ist. Bedeutet p jede beliebige in dem Modul k (also nicht in D) aufgehende ungerade Primzahl, so ist erforderlich, dass

$$\left(\frac{D}{p}\right) = +1$$

sei; ist diese Bedingung erfüllt, so hat die Congruenz $x^2 \equiv D$ in Bezug auf jeden Modulus von der Form p^π genau zwei incongruente Wurzeln. Ist daher der Modul k ungerade, und μ die Anzahl der von einander verschiedenen in k aufgehenden Primzahlen p, so ist

$$\sigma = 2^\mu.$$

Dasselbe ist der Fall, wenn der Modulus k das Doppelte einer ungeraden Zahl ist; denn die Congruenz $x^2 \equiv D \pmod{2}$ hat stets eine und nur eine Wurzel.

Ist aber k das Vierfache einer ungeraden Zahl, so ist ausser den früheren μ Bedingungen noch erforderlich, dass $D \equiv 1 \pmod{4}$ sei; da alsdann die Congruenz $x^2 \equiv D \pmod{4}$ zwei Wurzeln besitzt, so ist

$$\sigma = 2^{\mu+1}.$$

Ist endlich $k \equiv 0 \pmod{8}$, so ist ausser den früheren μ Bedingungen noch erforderlich, dass $D \equiv 1 \pmod{8}$ sei; da dann die Congruenz $x^2 \equiv D \pmod{2^\pi}$, wo $\pi \geqq 3$, stets vier Wurzeln hat, so ist in diesem Fall

$$\sigma = 2^{\mu+2}.$$

§. 38.

Bevor wir diesen Gegenstand verlassen, wollen wir noch eine Anwendung von dem soeben gewonnenen Resultate auf eine Verallgemeinerung des Wilson'schen Satzes (§. 27) machen. Setzen wir $D = 1$, so ergiebt sich, dass die Congruenz

$$x^2 \equiv 1 \pmod{k} \qquad (1)$$

für jeden Modul k möglich ist; die Anzahl σ ihrer Wurzeln ist $= 1$, wenn $k = 1$ oder $k = 2$; sie ist $= 2$, wenn k eine Potenz einer ungeraden Primzahl oder das Doppelte einer solchen Potenz oder $= 4$ ist; in allen übrigen Fällen ist σ durch 4 theilbar. Schliessen wir die Fälle $k = 1$ und $k = 2$ aus, so zerfallen die σ Wurzeln in $\frac{1}{2}\sigma$ Paare von Wurzeln ϱ und $-\varrho$; denn mit ϱ ist gleichzeitig auch $-\varrho$ eine Wurzel, und da ϱ relative Primzahl zu k, und folglich 2ϱ nicht $\equiv 0 \pmod{k}$ sein kann, so sind je zwei solche Wurzeln ϱ und $-\varrho$ auch incongruent. Das Product $\varrho \times (-\varrho) = -\varrho^2$ zweier solcher Wurzeln ist $\equiv -1$, und folglich ist das Product aller σ Wurzeln $\equiv +1$ oder -1, je nachdem σ durch 4 theilbar ist oder nicht.

Unter den $\varphi(k)$ Zahlen z, welche nicht grösser als k und relative Primzahlen zu k sind, finden sich zunächst die σ Wurzeln der Congruenz (1); die übrigen $\varphi(k) - \sigma$ dieser Zahlen z (wenn noch solche vorhanden sind) lassen sich in Paare von je zwei solchen Zahlen r und s zerlegen, deren Product $rs \equiv 1$ ist; denn zu jeder Zahl r gehört (nach §. 22) eine solche Zahl s und nur eine, und ausserdem kann s nicht $\equiv r$ sein, weil sonst $r^2 \equiv 1$, und folglich r eine der σ Wurzeln der Congruenz (1) wäre. Mithin ist auch das Product aller dieser $\varphi(k) - \sigma$ Zahlen $\equiv 1$.

Multiplicirt man daher alle $\varphi(k)$ Zahlen z mit einander, so wird das Product $\equiv -1$, wenn k Potenz einer ungeraden Primzahl oder das Doppelte einer solchen Potenz oder $= 4$ ist, in allen übrigen Fällen aber $\equiv +1$. (In den beiden ausgeschlossenen Fällen $k = 1$ und $k = 2$ ist $\varphi(k) = 1$, und die einzige Zahl $z \equiv \pm 1$.) Dies ist der verallgemeinerte Wilson'sche Satz*).

§. 39.

Nachdem in den vorhergehenden Paragraphen die erste der beiden in §. 32 aufgeworfenen Fragen ihre vollständige Beantwortung gefunden hat, wenden wir uns jetzt zu der zweiten ungleich interessanteren, aber auch schwierigern Aufgabe:

Alle Moduln k zu finden, von welchen eine gegebene Zahl D quadratischer Rest ist.

*) *Gauss: D. A.* art. 78.

Bevor wir zu der Lösung derselben übergehen, wollen wir erwähnen, dass man häufig, namentlich in den älteren Schriften, eine andere Ausdrucksweise vorfindet. Die Moduln k, für welche eine Congruenz $f(x) \equiv 0 \pmod{k}$ möglich ist, nennt man auch *Divisoren der Form* $f(x)$, weil es Zahlen x giebt, für welche die *Form* $f(x)$ durch einen solchen Modul k theilbar wird; die von uns gesuchten Zahlen k sind daher die Divisoren der Form $x^2 - D$; sie stimmen vollständig überein mit den Divisoren der *Form* $t^2 - Du^2$, in welcher t, u zwei unbestimmte ganze Zahlen bedeuten, die aber immer relative Primzahlen zu einander sein müssen. Dass wirklich jeder Divisor der Form $x^2 - D$ auch ein Divisor der Form $t^2 - Du^2$ ist, leuchtet unmittelbar ein, da die letztere in die erstere übergeht, wenn man $t = x$, $u = 1$ setzt. Umgekehrt, ist k Divisor der Form $t^2 - Du^2$, so ist u jedenfalls relative Primzahl zu k (denn ginge irgend eine Primzahl gleichzeitig in k und u auf, so müsste sie auch in t^2 und folglich auch in t aufgehen, gegen die Voraussetzung, dass t, u relative Primzahlen sind), und man kann folglich eine Zahl x finden, welche der Congruenz $ux \equiv t \pmod{k}$ genügt; da nun $t^2 - Du^2 \equiv 0 \pmod{k}$, so ist auch $u^2(x^2 - D) \equiv 0 \pmod{k}$ und folglich, da u^2 relative Primzahl zu k ist, auch $x^2 - D \equiv 0 \pmod{k}$, d. h. jeder Divisor k der Form $t^2 - Du^2$, in welcher t und u relative Primzahlen zu einander sind, ist auch Divisor der Form $x^2 - D$.

Das allgemeine Problem wird daher häufig auch so ausgedrückt: es sollen alle Divisoren der Form $t^2 - Du^2$ gefunden werden, in welcher D eine gegebene, t und u dagegen zwei unbestimmte ganze Zahlen bedeuten, die relative Primzahlen zu einander sind.

Wir beschränken uns auch hier auf solche (immer mit *positivem* Vorzeichen genommene) Moduln k, die relative Primzahlen zu D sind; da ferner nach den vorhergehenden Untersuchungen die Möglichkeit der Congruenz $x^2 \equiv D \pmod{k}$ nur von der Beschaffenheit der in k aufgehenden Primzahlen abhängt und für einen Modul von der Form 2^π immer leicht beurtheilt werden kann, so kommt es nur darauf an, alle ungeraden (in D nicht aufgehenden) Primzahlen p zu finden, von welchen D quadratischer Rest ist. Bedenken wir ferner, dass (nach §. 33) der quadratische Charakter einer Zahl D in Bezug auf einen solchen Modulus p nur von den in D enthaltenen Factoren abhängt, so werden wir in letzter Instanz auf folgendes Problem geführt:

Alle ungeraden Primzahlen p zu finden, für welche irgend eine der drei Congruenzen

$$x^2 \equiv -1, \quad x^2 \equiv 2, \quad x^2 \equiv q \pmod{p}$$

möglich ist, wo q irgend eine gegebene positive ungerade Primzahl bedeutet.

§. 40.

Die Auffindung aller ungeraden Primzahlen p, für welche die Congruenz

$$x^2 \equiv -1 \pmod{p}$$

möglich ist, bietet keine Schwierigkeit mehr dar. Denn da (nach §. 33) allgemein

$$\left(\frac{D}{p}\right) \equiv D^{\frac{p-1}{2}} \pmod{p}$$

ist, so erhält man speciell

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und folglich auch

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

In Worten lautet dieser wichtige Satz*) folgendermaassen:

Die Zahl -1 *ist quadratischer Rest aller Primzahlen von der Form* $4n+1$, *dagegen quadratischer Nichtrest aller Primzahlen von der Form* $4n+3$.

Dasselbe Resultat erhält man auch auf folgendem Wege. Ist die Congruenz $x^2 \equiv -1 \pmod{p}$ möglich, und x eine Wurzel derselben, so folgt hieraus durch Potenzirung

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und hieraus (nach dem Fermat'schen Satze §. 19) $(-1)^{\frac{p-1}{2}} = 1$ also $p = 4n+1$; d. h. die Zahl -1 ist quadratischer Nichtrest von allen Primzahlen von der Form $4n+3$. Ist umgekehrt p von der Form $4n+1$, so ist $x^{p-1}-1$ algebraisch theilbar durch x^4-1, also auch durch x^2+1; es ist folglich

$$x^{p-1} - 1 = (x^2+1)\,\psi(x),$$

---

*) *Euler: Demonstratio theorematis Fermatiani, omnem numerum primum formae* $4n+1$ *esse summam duorum quadratorum*, Nov. Comm. Petrop. V, p. 3.

wo $\psi(x)$ ein Polynom mit ganzen Coefficienten bedeutet; da nun (nach dem Fermat'schen Satze §. 19) die linke Seite dieser Gleichung für $p-1$ incongruente Werthe von x congruent Null wird, so wird (nach §. 26) auch x^2+1 für zwei incongruente Werthe von x congruent Null *), d. h. die Zahl -1 ist quadratischer Rest von allen Primzahlen von der Form $4n+1$. Der Satz ist also von Neuem bewiesen.

§. 41.

Wir gehen nun zu der Lösung der zweiten Aufgabe über, welche sich auf die Congruenz

$$x^2 \equiv 2 \pmod{p}$$

bezieht. *Fermat* hat, wahrscheinlich durch Induction, folgendes, zuerst von *Lagrange* **) bewiesenes, Resultat gefunden:

Die Zahl 2 ist quadratischer Rest aller Primzahlen von einer der beiden Formen $8n+1$ oder $8n+7$, dagegen Nichtrest aller Primzahlen von einer der beiden Formen $8n+3$ oder $8n+5$.

Wir beweisen zuerst den zweiten Theil des Satzes, dass nämlich 2 Nichtrest aller Primzahlen p von der Form $8n\pm 3$ ist. Offenbar ist derselbe für $p=3$ richtig, denn nur die Zahl 1 ist Rest von 3. Gesetzt nun, der Satz wäre nicht allgemein gültig, so müsste es doch eine *kleinste* Primzahl p von der Form $8n\pm 3$ geben, für welche er unrichtig würde, für welche also die Congruenz

$$x^2 \equiv 2 \pmod{p}$$

möglich würde. Hierin kann man immer die Wurzel x kleiner als p und ungerade voraussetzen, denn wenn x gerade ist, so ist die andere Wurzel $x'=p-x$ ungerade. Wir können daher

$$x^2-2=pf$$

setzen, wo f positiv und kleiner als p ist; da ferner x^2 von der Form $8n+1$, also pf von der Form $8n-1$, und folglich f von der Form $8n\mp 3$ ist, so hat die Zahl f mindestens einen Primfactor p' von einer der Formen $8n+3$ oder $8n-3$; denn ein Product aus lauter Factoren von der Form $8n\pm 1$ würde wieder

---

*) Man findet auch leicht mit Hülfe des Wilson'schen Satzes (§. 27), dass diese Wurzeln $\equiv \pm 1 \,.\, 2 \,.\, 3 \ldots \frac{1}{2}(p-1)$ sind.

**) *Recherches d'Arithmétique*, Nouv. Mém. de l'Acad. de Berlin. 1775. p. 349, 351.

dieselbe Form $8n \pm 1$ haben. Für diese Primzahl p', die jedenfalls $< p$ ist, würde dann ebenfalls $x^2 \equiv 2 \pmod{p'}$ sein; allein dies streitet mit unserer Voraussetzung, dass p die kleinste in der Form $8n \pm 3$ enthaltene Primzahl ist, von welcher die Zahl 2 quadratischer Rest ist. Mithin ist diese Voraussetzung überhaupt unzulässig, und es folgt, dass stets

$$\left(\frac{2}{p}\right) = -1 \text{ ist, wenn } p = 8n \pm 3.$$

Wir wollen jetzt zweitens beweisen, dass die Zahl 2 quadratischer Rest aller Primzahlen p von der Form $8n + 7$ ist; da nun (nach §. 40) -1 quadratischer Nichtrest aller dieser Primzahlen ist, so haben wir nur zu zeigen, dass die Zahl -2 ebenfalls Nichtrest aller dieser Primzahlen ist; statt dessen stellen wir uns die allgemeinere Aufgabe zu beweisen, dass -2 Nichtrest von allen in den beiden Formen $8n + 5$, $8n + 7$ enthaltenen Primzahlen ist, obgleich dies für die Primzahlen der Form $8n + 5$, von welchen (nach §. 40) -1 quadratischer Rest ist, schon im Vorhergehenden geschehen ist. Zunächst bemerken wir wieder, dass der Satz für die kleinste in einer dieser Formen enthaltene Primzahl 5 in der That richtig ist. Wenn nun der Satz nicht allgemein gültig ist, so sei p die kleinste ihm nicht gehorchende Primzahl, so dass also eine Zahl x existirt, für welche

$$x^2 + 2 \equiv 0 \pmod{p}$$

ist; auch hier können wir wieder annehmen, dass x kleiner als p und ungerade ist, so dass, wenn wir

$$x^2 + 2 = pf$$

setzen, die Zahl f positiv, ungerade und kleiner als p ausfällt. Da ferner $x^2 + 2 \equiv 3 \pmod{8}$ und $p \equiv 5$ oder $\equiv 7 \pmod{8}$ ist, so muss f entsprechend $\equiv 7$ oder $\equiv 5 \pmod{8}$ sein; und da ein Product aus lauter Factoren von den Formen $8n + 1$, oder $8n + 3$ stets wieder eine dieser Formen, niemals eine der Formen $8n + 5$ oder $8n + 7$ hat, so muss die Zahl f mindestens einen Primfactor p' von einer der Formen $8n + 7$, $8n + 5$ haben, für welchen der Satz ebenfalls unrichtig ist, da $x^2 + 2 \equiv 0 \pmod{p'}$ ist; allein, da $p' < p$, so streitet dies mit der Annahme, dass p die kleinste dem Satze nicht gehorchende Primzahl ist. Also ist die Annahme überhaupt nicht zulässig und folglich der Satz allgemeingültig, dass

$$\left(\frac{-2}{p}\right) = -1 \text{ für } p = 8n + 5 \text{ oder } = 8n + 7,$$

d. h. dass

$$\left(\frac{2}{p}\right) = -1 \text{ für } p = 8n + 5$$
$$\left(\frac{2}{p}\right) = +1 \text{ für } p = 8n + 7$$

ist.

Es bleibt jetzt nur noch zu beweisen übrig, dass 2 quadratischer Rest von allen Primzahlen p von der Form $8n+1$ ist; hierauf ist die vorhergehende Methode aus dem Grunde nicht anwendbar, weil die Annahme des Gegentheils sich nicht in Form einer Congruenz darstellen lässt, die dann zur Auffindung des Widerspruchs benutzt werden könnte. Allein in diesem Falle kann man direct, wie folgt, verfahren; da $p = 8n+1$ ist, so hat die Function $x^{p-1} - 1$ den Divisor $x^8 - 1$, also auch den Factor $x^4 + 1$, und hieraus folgt nach einem frühern Satze (§. 26), dass die Congruenz

$$x^4 + 1 \equiv 0 \pmod{p}$$

Wurzeln hat; ist nun x eine solche, so ist

$$x^4 + 1 = (x^2 \pm 1)^2 \mp 2x^2 \equiv 0 \pmod{p},$$

also

$$(x^2 \pm 1)^2 \equiv \pm 2x^2 \pmod{p};$$

es ist daher $\pm 2x^2$ und folglich auch ± 2 quadratischer Rest von p; in Zeichen

$$\left(\frac{\pm 2}{p}\right) = 1, \text{ wenn } p = 8n + 1.$$

Hiermit ist der Satz in allen seinen Theilen bewiesen; wir können denselben n der einen Gleichung

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

zusammenfassen; denn je nachdem $p = 8n \pm 1$, oder $p = 8n \pm 3$ ist, wird $\frac{1}{8}(p^2 - 1)$ eine gerade oder ungerade Zahl.

§. 42.

Wir kommen nun zu der Untersuchung der dritten Frage: *von welchen ungeraden Primzahlen p ist die gegebene ungerade*

Primzahl q quadratischer Rest? Die vollständige Antwort hierauf wird durch einen der wichtigsten und interessantesten Sätze der Zahlentheorie gegeben, welcher seines eigenthümlichen Charakters wegen den Namen des *Reciprocitäts-Satzes* erhalten hat. Man kann ihn folgendermaassen aussprechen:

Sind p und q zwei positive ungerade Primzahlen, von denen mindestens eine die Form $4n+1$ hat, so ist q quadratischer Rest oder Nichtrest von p, je nachdem p quadratischer Rest oder Nichtrest von q ist; haben aber beide Primzahlen p und q die Form $4n+3$, so ist q quadratischer Rest oder Nichtrest von p, je nachdem p quadratischer Nichtrest oder quadratischer Rest von q ist.

Offenbar lässt sich dieser Satz durch die für beide Fälle gültige Gleichung

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ausdrücken; denn sobald mindestens eine der beiden Primzahlen p oder q die Form $4n+1$ hat, so ist die entsprechende der beiden Zahlen $\frac{1}{2}(p-1)$ oder $\frac{1}{2}(q-1)$, und folglich auch ihr Product $\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ eine gerade Zahl, so dass

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1, \text{ d. h. } \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

ist, worin der erste Fall seinen Ausdruck findet; sind dagegen beide Primzahlen p und q von der Form $4n+3$, so sind auch beide Zahlen $\frac{1}{2}(p-1)$ und $\frac{1}{2}(q-1)$, und folglich auch ihr Product $\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ ungerade, so dass

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1, \text{ d. h. } \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$$

wird, worin der zweite Theil des Satzes ausgedrückt ist.

Ist z. B. $p=3$, $q=5$, so ist p quadratischer Nichtrest von q und gleichzeitig q quadratischer Nichtrest von p, in Zeichen

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = -1.$$

Ist ferner $p=3$, $q=13$, so ist p quadratischer Rest von q und gleichzeitig q quadratischer Rest von p, in Zeichen

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = +1.$$

Ist dagegen $p=3$, $q=7$, so ist p quadratischer Nichtrest von q und gleichzeitig q quadratischer Rest von p, in Zeichen

$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -1.$$

Dieser Satz wurde zuerst von *Legendre* durch Induction gefunden und ausgesprochen; allein erst *Gauss* hat denselben vollständig bewiesen, ja er hat nach einander sechs auf ganz verschiedenen Grundgedanken beruhende Beweise*) von diesem Satze gegeben, den er in etwas anderer Form aussprach und seiner Wichtigkeit wegen das *Theorema fundamentale* in der Theorie der quadratischen Reste nannte. Wir folgen hier zunächst dem *dritten* dieser sechs Beweise, der sich auf ein Lemma stützt, durch welches das Euler'sche Kriterium (§. 33) über den Charakter einer Zahl D in Bezug auf die Primzahl p in ein anderes umgeformt wird.

§. 43.

Wir haben früher (§. 33) gesehen, dass eine durch p nicht theilbare Zahl D quadratischer Rest oder Nichtrest von p ist, je nachdem

$$D^{\frac{p-1}{2}} \equiv +1 \text{ oder } \equiv -1 \pmod{p}$$

ist; betrachten wir nun die Producte

$$D, \quad 2D, \quad 3D \ldots \tfrac{1}{2}(p-1)D$$

aus dieser Zahl D und aus den ersten $\frac{1}{2}(p-1)$ ganzen positiven Zahlen, so werden die kleinsten positiven Reste

$$r_1, \quad r_2, \quad r_3 \ldots r_{\frac{p-1}{2}}$$

derselben, nach dem Modulus p genommen, erstens sämmtlich verschieden von einander und kleiner als p sein, und keiner von ihnen kann gleich Null sein. Wir theilen nun diese $\frac{1}{2}(p-1)$ Reste in zwei Abtheilungen, je nachdem sie grösser oder kleiner als $\frac{1}{2}p$ sind, und bezeichnen die erstern, deren Anzahl $= \mu$ sei, mit

$$\alpha_1, \quad \alpha_2 \ldots \alpha_\mu,$$

*) *D. A.* artt. 125—145. — *D. A.* art. 262. — *Theorematis arithmetici demonstratio nova.* 1808. — *Summatio quarumdam serierum singularium.* 1808. — *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae.* 1817. — Vergl. §§. 48—51, 115.

die übrigen Reste, welche kleiner als $\frac{1}{2}p$ sind, und deren Anzahl $\lambda = \frac{1}{2}(p-1) - \mu$ ist, mit

$$\beta_1, \quad \beta_2 \ldots \beta_\lambda.$$

Nimmt man nun von den erstern μ Resten ihre Ergänzungen zur Zahl p, also die Zahlen

$$p-\alpha_1, \quad p-\alpha_2 \ldots p-\alpha_\mu,$$

so liegen dieselben, ebenso wie die λ Zahlen $\beta_1, \beta_2 \ldots \beta_\lambda$, auch zwischen den Grenzen 0 und $\frac{1}{2}p$; ausserdem sind sie alle von einander verschieden; endlich lässt sich aber auch zeigen, dass sie von den λ Zahlen $\beta_1, \beta_2 \ldots \beta_\lambda$ verschieden sind; denn wäre z. B. $p-\alpha = \beta$, also $\alpha + \beta = p \equiv 0$ (mod. p), so müsste auch, wenn α der Rest von sD, β der Rest von tD ist,

$$sD + tD = (s+t)D \equiv 0 \pmod{p}$$

und folglich $s+t$ durch p theilbar sein; allein da jede der beiden Zahlen s und t zwischen 0 und $\frac{1}{2}p$ liegt, so liegt $s+t$ zwischen 0 und p (mit Ausschluss dieser beiden Grenzen); es kann daher $s+t$ nicht theilbar durch p, und folglich auch nicht $p-\alpha = \beta$ sein.

Mithin haben die folgenden $\frac{1}{2}(p-1)$ Zahlen

$$p-\alpha_1, \quad p-\alpha_2 \ldots p-\alpha_\mu; \quad \beta_1, \quad \beta_2 \ldots \beta_\lambda$$

lauter von einander verschiedene Werthe, und da sie ihrem Werth nach zwischen 0 und $\frac{1}{2}p$ liegen, so müssen sie im Complex genommen identisch mit den $\frac{1}{2}(p-1)$ Zahlen

$$1, \quad 2, \quad 3 \ldots \tfrac{1}{2}(p-1)$$

sein, so dass ihr Product

$$(p-\alpha_1)(p-\alpha_2)\ldots(p-\alpha_\mu)\,\beta_1\beta_2\ldots\beta_\lambda = 1.2.3\cdots\tfrac{1}{2}(p-1)$$

ist. Werfen wir hieraus die Multipla von p weg, so erhalten wir die Congruenz

$$(-1)^\mu\,\alpha_1\alpha_2\ldots\alpha_\mu.\beta_1\beta_2\ldots\beta_\lambda \equiv 1.2.3\cdots\tfrac{1}{2}(p-1) \pmod{p};$$

da nun andererseits

$$\alpha_1\alpha_2\ldots\alpha_\mu.\beta_1\beta_2\ldots\beta_\lambda \equiv 1.2\cdots\tfrac{1}{2}(p-1)\,D^{\frac{p-1}{2}} \pmod{p}$$

ist, so folgt hieraus, dass

$$(-1)^\mu.1.2\cdots\tfrac{1}{2}(p-1).D^{\frac{p-1}{2}} \equiv 1.2.3\cdots\tfrac{1}{2}(p-1) \pmod{p}$$

und also auch

$$D^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p}$$

oder, was dasselbe sagt, dass

$$\left(\frac{D}{p}\right) = (-1)^\mu$$

ist. Hierin besteht die Umformung des Kennzeichens, welches darüber entscheidet, ob eine Zahl D quadratischer Rest oder Nichtrest der ungeraden Primzahl p ist:

Man braucht nur nachzusehen, ob die Anzahl μ der kleinsten positiven Reste der Zahlen

$$D,\ 2D,\ 3D \ldots \tfrac{1}{2}(p-1)D,$$

die grösser als $\frac{1}{2}p$ ausfallen, gerade oder ungerade ist; je nachdem das Erstere oder Letztere eintritt, ist D quadratischer Rest oder quadratischer Nichtrest von p.

Mit Hülfe dieses Satzes ist man schon im Stande, für jedes wirklich gegebene D die Formen für die Primzahlen aufzustellen, von welchen D Rest oder Nichtrest ist. Um dies deutlicher zu zeigen, betrachten wir den allerdings schon früher (§. 41) vollständig durchgeführten Fall $D = 2$. Bilden wir die Zahlen

$$2,\ 4,\ 6 \ldots (p-1),$$

so ist jede derselben auch ihr eigener kleinster positiver Rest in Bezug auf den Modulus p, und die Anzahl μ derjenigen dieser Zahlen, welche $> \frac{1}{2}p$ sind, wird durch die Bedingungen

$$p - 1 - 2\mu < \tfrac{1}{2}p < p + 1 - 2\mu \quad \text{oder} \quad \frac{p-2}{4} < \mu < \frac{p+2}{4}$$

bestimmt; bezeichnen wir daher allgemein mit $[x]$ die grösste in der reellen Zahl x enthaltene *ganze* Zahl, so dass stets $0 \leqq x - [x] < 1$ ist, so erhalten wir

$$\mu = \left[\frac{p+2}{4}\right].$$

Je nachdem nun p von einer der Formen $8n+1$, $8n+3$, $8n+5$, $8n+7$ ist, wird $\mu = 2n$, $2n+1$, $2n+1$, $2n+2$; es ist daher μ gerade und folglich

$$\left(\frac{2}{p}\right) = +1, \quad \text{wenn} \quad p \equiv \pm 1 \pmod{8};$$

und μ ist ungerade, also

$$\left(\frac{2}{p}\right) = -1, \quad \text{wenn} \quad p \equiv \pm 3 \pmod{8}.$$

Auf diese Weise finden wir also eine vollständige Bestätigung des Resultats unserer frühern Untersuchung (§. 41), und ganz ebenso würde sich für jeden speciellen Werth von D die Untersuchung führen lassen, z. B. für die nächstliegenden Fälle $D = -1$, $D = 3$, $D = 5$ u. s. w.

§. 44.

Wir verlassen diese Anwendungen auf specielle Fälle und wenden uns zu einer weitern Umformung, bei welcher wir der spätern Bezeichnung wegen q statt D schreiben wollen. Bezeichnen wir wieder mit $[x]$ die grösste in dem Werth x enthaltene ganze Zahl, und setzen wir zur Abkürzung $p = 2p' + 1$, so können wir

$$q = p\left[\frac{q}{p}\right] + r_1$$

$$2q = p\left[\frac{2q}{p}\right] + r_2$$

$$\cdots\cdots\cdots\cdots$$

$$p'q = p\left[\frac{p'q}{p}\right] + r_{p'}$$

setzen, wo wie früher (§. 43)

$$r_1, \quad r_2 \ldots r_{p'}$$

zwischen den Grenzen 0 und p liegen; theilen wir wieder diese kleinsten Reste in zwei Abtheilungen

$$\alpha_1, \quad \alpha_2 \ldots \alpha_\mu$$

und

$$\beta_1, \quad \beta_2 \ldots \beta_\lambda,$$

von denen die ersteren $> \frac{1}{2}p$, die letzteren $< \frac{1}{2}p$ sind, und bezeichnen wir mit A die Summe der μ ersteren, mit B die Summe der λ letzteren, ferner mit M die Summe

$$M = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \cdots + \left[\frac{p'q}{p}\right],$$

so folgt durch Addition der vorstehenden Gleichungen

$$\frac{p^2 - 1}{8} q = pM + A + B;$$

da nun (nach §. 43) der Complex der Zahlen

$$p-\alpha_1,\ p-\alpha_2\ldots p-\alpha_\mu;\ \beta_1,\beta_2\ldots\beta_\lambda$$

mit dem Complex der Zahlen

$$1, 2, 3\ldots\frac{p-1}{2}$$

vollständig übereinstimmt, so ist ihre Summe

$$\frac{p^2-1}{8}=\mu p-A+B;$$

zieht man diese Gleichung von der vorhergehenden ab, so erhält man

$$\frac{p^2-1}{8}(q-1)=(M-\mu)p+2A.$$

Nun kommt es uns lediglich darauf an, zu erfahren, ob μ gerade oder ungerade ist; lassen wir daher alle Multipla von 2 fort, so erhalten wir, da $p\equiv-1$ (mod. 2) gesetzt werden kann,

$$\mu\equiv M+\frac{p^2-1}{8}(q-1)\ (\text{mod. } 2).$$

Je nachdem daher die zur Rechten befindliche Zahl gerade oder ungerade ist, wird q quadratischer Rest oder Nichtrest von p sein. Nehmen wir daher z.B. wieder den Fall $q=2$, so ergiebt sich unmittelbar $M=0$, also

$$\mu\equiv\frac{p^2-1}{8}\ (\text{mod. } 2),$$

folglich

$$\left(\frac{2}{p}\right)=(-1)^\mu=(-1)^{\frac{p^2-1}{8}};$$

dies ist aber genau die schon früher (§. 41) aufgestellte Formel.

Von jetzt an wollen wir die Untersuchung nur noch unter der Voraussetzung fortführen, dass q eine *ungerade*, also $q-1$ eine gerade Zahl ist; dann ist also

$$\mu\equiv M\ (\text{mod. } 2),\quad \left(\frac{q}{p}\right)=(-1)^M;$$

und es reducirt sich daher die ganze Frage darauf, zu entscheiden, ob die oben mit M bezeichnete Summe *gerade* oder *ungerade* ist.

Um dies weiter zu untersuchen, machen wir die fernere Annahme, es sei q *positiv* und *kleiner als* p. Dann leuchtet zunächst

ein, dass jedes Glied in der Reihe M höchstens um eine Einheit grösser ist als das unmittelbar vorhergehende, weil der Unterschied von zwei auf einander folgenden Brüchen

$$\frac{sq}{p} \quad \text{und} \quad \frac{(s+1)q}{p}$$

< 1 ist, und folglich höchstens *eine* ganze Zahl zwischen beiden liegen kann; da ferner der letzte Bruch

$$\frac{p'q}{p} = \frac{(p-1)q}{2p} = \frac{q-1}{2} + \frac{p-q}{2p}$$

ist, so ist der Werth des letzten Gliedes in der obigen Reihe

$$\left[\frac{p'q}{p}\right] = \frac{q-1}{2} = q'.$$

Mithin kommen in der Summe M nach und nach Glieder vor, welche die Werthe $0, 1, 2 \,.\,. \, q'$ besitzen; wir suchen nun gerade die Stellen auf, wo zwei auf einander folgende Glieder

$$\left[\frac{sq}{p}\right] \quad \text{und} \quad \left[\frac{(s+1)q}{p}\right]$$

wirklich um eine Einheit verschieden sind, so dass, wenn t irgend eine der Zahlen $1, 2 \ldots q'$ bedeutet,

$$\frac{sq}{p} < t < \frac{(s+1)q}{p}$$

wird (da q relative Primzahl zu p, und $s < p$ ist, so kann keiner der Brüche $sq:p$ eine ganze Zahl sein); hieraus folgt aber

$$s < \frac{tp}{q} < s+1, \quad \text{also} \quad s = \left[\frac{tp}{q}\right],$$

und folglich giebt es in der Reihe M jedesmal

$$\left[\frac{tp}{q}\right] - \left[\frac{(t-1)p}{q}\right]$$

Glieder, welche den Werth $(t-1)$ haben; und die Anzahl der letzten Glieder, welche den Werth q' haben, ist offenbar

$$p' - \left[\frac{q'p}{q}\right].$$

Multiplicirt man nun jedesmal die Anzahl einer solchen Gruppe von Gliedern, welche einen und denselben Werth haben, mit diesem Werth, so muss die Summe aller dieser Producte $= M$ werden Dies giebt

$$0\cdot\left[\frac{p}{q}\right]+1\cdot\left(\left[\frac{2p}{q}\right]-\left[\frac{p}{q}\right]\right)+2\cdot\left(\left[\frac{3p}{q}\right]-\left[\frac{2p}{q}\right]\right)+\cdots$$
$$+(q'-1)\cdot\left(\left[\frac{q'p}{q}\right]-\left[\frac{(q'-1)p}{q}\right]\right)+q'\cdot\left(\frac{p-1}{2}-\left[\frac{q'p}{q}\right]\right)$$
$$=-\left[\frac{p}{q}\right]-\left[\frac{2p}{q}\right]-\cdots-\left[\frac{q'p}{q}\right]+q'\cdot\frac{p-1}{2}.$$

Setzen wir daher

$$N=\left[\frac{p}{q}\right]+\left[\frac{2p}{q}\right]+\cdots+\left[\frac{q'p}{q}\right],$$

so erhalten wir das Resultat

$$M+N=\frac{p-1}{2}\cdot\frac{q-1}{2},$$

welches offenbar für *je zwei positive ungerade relative Primzahlen* p, q gültig ist; denn bei der Ableitung ist weiter Nichts vorausgesetzt, und da das Resultat vollkommen symmetrisch in Bezug auf die beiden Zahlen p, q ist, von welchen doch eine jedenfalls die kleinere sein muss, so ist auch die bei dem Beweise gemachte Annahme, es sei $p > q$, erlaubt.

Hiermit ist nun zwar die Summe M nicht selbst gefunden, sondern nur auf die Summe N zurückgeführt; aber dies genügt vollständig, um den Reciprocitäts-Satz daraus abzuleiten. Oben ist gezeigt, dass, wenn p eine positive ungerade Primzahl, und q irgend eine durch p nicht theilbare ungerade Zahl bedeutet, stets

$$\left(\frac{q}{p}\right)=(-1)^M$$

st; nehmen wir daher jetzt ferner an, dass q ebenfalls eine positive ungerade Primzahl ist, so wird ebenso

$$\left(\frac{p}{q}\right)=(-1)^N,$$

und folglich, mit Rücksicht auf den so eben bewiesenen Satz,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{M+N}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

worin der Reciprocitäts-Satz besteht.

§. 45.

Wir betrachten zunächst ein Beispiel, um die Nützlichkeit des Reciprocitätssatzes für die Beurtheilung der Möglichkeit einer Congruenz von der Form

$$x^2 \equiv D \pmod{p}$$

nachzuweisen. Nehmen wir die Congruenz

$$x^2 \equiv 365 \pmod{1847},$$

so ist der Werth des Symbols

$$\left(\frac{365}{1847}\right)$$

zu ermitteln. Zunächst zerlegen wir 365 in Primfactoren, obgleich dies, wie wir später sehen werden, nicht nothwendig ist.

Aus dieser Zerlegung $365 = 5 . 73$ folgt unmittelbar

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right).$$

Da ferner 5 von der Form $4n + 1$ ist, so ergiebt sich aus dem Reciprocitätssatze

$$\left(\frac{5}{1847}\right) = \left(\frac{1847}{5}\right)$$

und also, da $1847 \equiv 2 \pmod{5}$ ist,

$$\left(\frac{5}{1847}\right) = \left(\frac{2}{5}\right) = -1$$

nach §. 41; da ferner auch 73 von der Form $4n + 1$ ist, so folgt wieder aus dem Reciprocitätssatze, und weil $1847 \equiv 22 \pmod{73}$ ist,

$$\left(\frac{73}{1847}\right) = \left(\frac{1847}{73}\right) = \left(\frac{22}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{11}{73}\right);$$

nun ist aber $73 \equiv 1 \pmod{8}$, also (nach §. 41)

$$\left(\frac{2}{73}\right) = 1, \quad \text{folglich} \quad \left(\frac{73}{1847}\right) = \left(\frac{11}{73}\right);$$

nach dem Reciprocitätssatze ist aber wieder

$$\left(\frac{11}{73}\right) = \left(\frac{73}{11}\right) = \left(\frac{7}{11}\right),$$

und da beide Primzahlen 7 und 11 von der Form $4n + 3$ sind, so ist abermals nach dem Reciprocitätssatze

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1,$$

folglich

$$\left(\frac{73}{1847}\right) = \left(\frac{11}{73}\right) = \left(\frac{7}{11}\right) = -1$$

und also endlich

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right) = (-1)(-1) = +1,$$

es ist also 365 quadratischer Rest der Primzahl 1847, d. h. die oben vorgelegte Congruenz ist möglich; und in der That ist

$$(\pm 496)^2 = 246016 = 365 + 133 \,.\, 1847.$$

§. 46.

Der in dem eben behandelten Beispiel angewendete Algorithmus, welcher auch bei jedem ähnlichen Beispiel nach einer endlichen Anzahl von Operationen zum Ziele führt, lässt sich im Allgemeinen bedeutend abkürzen, wenn man sich einer zuerst von *Jacobi* *) in die Zahlentheorie eingeführten Verallgemeinerung des Legendre'schen Symbols bedient; da der Gebrauch dieses Zeichens auch für unsere späteren Untersuchungen unerlässlich ist, so beschäftigen wir uns zunächst mit der Erklärung desselben und den Gesetzen, denen es gehorcht.

Es sei die *ungerade* Zahl P in ihre Primzahlfactoren p, p', p'' u. s. w. zerlegt, also

$$P = p p' p'' \ldots$$

und m irgend eine *relative Primzahl* zu P, so setzen wir mit *Jacobi*

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots;$$

offenbar ist der Werth dieses Symbols $= +1$ oder $= -1$, je nachdem die Anzahl derjenigen Primfactoren $p, p', p'' \ldots$, von welchen m quadratischer Nichtrest ist, gerade oder ungerade ist. Wenn m

*) Monatsbericht der Berliner Akademie. 1837.

quadratischer Rest von P, und also auch von jeder einzelnen der Primzahlen $p, p', p'' \ldots$ ist, so ist

$$\left(\frac{m}{p}\right) = \left(\frac{m}{p'}\right) = \left(\frac{m}{p''}\right) \cdots = 1,$$

und folglich auch

$$\left(\frac{m}{P}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right) \cdots = 1;$$

aber man darf diesen Satz durchaus nicht umkehren; sobald nämlich die Zahl m von zweien der Primfactoren $p, p', p'' \ldots$ (oder von vier, von sechs u. s. w.) quadratischer Nichtrest ist, so hat das Symbol den Werth $+1$, und doch ist m quadratischer Nichtrest von P. Im einfachsten Fall, wo P selbst eine ungerade Primzahl ist, stimmt die Bedeutung des Zeichens offenbar mit der frühern überein. Der Vollständigkeit wegen wollen wir ferner festsetzen, dass, wenn $P = 1$, das Symbol immer die positive Einheit bedeuten soll.

Aus dieser Definition des Zeichens ergeben sich nun folgende Sätze:

1. Ist m relative Primzahl gegen jede der beiden ungeraden Zahlen P und Q, also auch gegen die ungerade Zahl PQ, so ist

$$\left(\frac{m}{P}\right)\left(\frac{m}{Q}\right) = \left(\frac{m}{PQ}\right);$$

denn, wenn

$$P = pp'p'' \ldots$$
$$Q = qq'q'' \ldots$$

ist, wo $p, p' \ldots q, q' \ldots$ lauter Primzahlen bedeuten, so ist

$$\left(\frac{m}{PQ}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right) \cdots \left(\frac{m}{q}\right)\left(\frac{m}{q'}\right)\left(\frac{m}{q''}\right) \cdots$$
$$= \left(\frac{m}{P}\right)\left(\frac{m}{Q}\right).$$

2. Sind die Zahlen $l, m, n \ldots$ relative Primzahlen gegen die ungerade Zahl P, so ist

$$\left(\frac{l}{P}\right)\left(\frac{m}{P}\right)\left(\frac{n}{P}\right) \cdots = \left(\frac{lmn \ldots}{P}\right);$$

denn, wenn wieder

$$P = pp'p'' \ldots$$

ist, so ist

$$\left(\frac{l}{P}\right)=\left(\frac{l}{p}\right)\left(\frac{l}{p'}\right)\left(\frac{l}{p''}\right)\cdots$$
$$\left(\frac{m}{P}\right)=\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots$$
$$\left(\frac{n}{P}\right)=\left(\frac{n}{p}\right)\left(\frac{n}{p'}\right)\left(\frac{n}{p''}\right)\cdots$$

u. s. w.

Da nun ferner, wie früher (§. 33) bewiesen ist,

$$\left(\frac{l}{p}\right)\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\cdots=\left(\frac{l\,m\,n\cdots}{p}\right)$$

ist, und Aehnliches für die anderen Primfactoren p', p'' u. s. w. gilt, so erhält man durch Multiplication der vorangehenden Gleichungen

$$\left(\frac{l}{P}\right)\left(\frac{m}{P}\right)\left(\frac{n}{P}\right)\cdots=\left(\frac{lmn\ldots}{p}\right)\left(\frac{lmn\ldots}{p'}\right)\left(\frac{lmn\ldots}{p''}\right)\cdots,$$

worin der zu beweisende Satz besteht.

3. Ist m relative Primzahl zu der ungeraden Zahl P und $m \equiv m'$ (mod. P), also auch m' relative Primzahl zu P, so ist

$$\left(\frac{m}{P}\right)=\left(\frac{m'}{P}\right);$$

denn, wenn $P = pp'p'' \ldots$ ist, so ist auch

$$m \equiv m' \text{ (mod. } p), \quad m \equiv m' \text{ (mod. } p'),$$

u. s. w., also

$$\left(\frac{m}{p}\right)=\left(\frac{m'}{p}\right),\quad \left(\frac{m}{p'}\right)=\left(\frac{m'}{p'}\right),$$

u. s. w., und folglich

$$\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\cdots=\left(\frac{m'}{p}\right)\left(\frac{m'}{p'}\right)\cdots,$$

was zu beweisen war. —

4. Die beiden letzten Sätze zeigen, dass das verallgemeinerte Symbol denselben Gesetzen gehorcht wie das einfache; wir wollen nun zeigen, dass auch die Werthe der Symbole

$$\left(\frac{-1}{P}\right),\quad \left(\frac{2}{P}\right)$$

nach den früheren Regeln zu bestimmen sind, und endlich, dass auch ein dem frühern ganz analoger Reciprocitätssatz Statt findet; um

aber den Gang der Beweise nicht zu unterbrechen, schicken wir folgende Bemerkungen voraus. Ist

$$R = r' r'' r''' \ldots$$

eine beliebige ungerade Zahl, so sind $r'-1$, $r''-1$, $r'''-1 \ldots$ lauter gerade Zahlen, und folglich ist jedes Product aus zweien oder mehreren dieser Differenzen $\equiv 0 \pmod{4}$; bringt man daher R in die Form

$$R = (1 + (r'-1))\,(1 + (r''-1))\,(1 + (r'''-1)) \ldots$$

und führt die Multiplication aus, so ergiebt sich

$$R \equiv 1 + (r'-1) + (r''-1) + (r'''-1) + \cdots \pmod{4};$$

oder kürzer

$$\frac{R-1}{2} \equiv \Sigma \frac{r-1}{2} \pmod{2},$$

wo das Summenzeichen sich auf den Buchstaben r bezieht, der die einzelnen Factoren r', r'', $r''' \ldots$ durchlaufen muss.

Auf ganz ähnliche Weise ergiebt sich aus denselben Voraussetzungen noch ein zweites Lemma; es ist nämlich $r^2 \equiv 1 \pmod{8}$ und folglich

$$R^2 = (1 + (r'^2-1))\,(1 + (r''^2-1))\,(1 + (r'''^2-1)) \ldots$$
$$\equiv 1 + \Sigma\,(r^2-1) \pmod{64},$$

also

$$\frac{R^2-1}{8} \equiv \Sigma \frac{r^2-1}{8} \pmod{8}$$

und um so mehr

$$\frac{R^2-1}{8} \equiv \Sigma \frac{r^2-1}{8} \pmod{2}.$$

Nach diesen Vorbemerkungen kehren wir zu unserm Gegenstande zurück.

5. Ist P eine positive ungerade Zahl, so ist

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

Denn wenn P das Product aus den positiven Primzahlen p', p'', $p''' \ldots$ ist, so ist

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p'}\right)\left(\frac{-1}{p''}\right)\left(\frac{-1}{p'''}\right) \cdots = (-1)^{\Sigma\frac{p-1}{2}},$$

wo der Summationsbuchstabe p alle Primfactoren p', p'', $p''' \ldots$ durchlaufen muss; da nun nach dem ersten Lemma 4.

$$\Sigma \frac{p-1}{2} \equiv \frac{P-1}{2} \pmod{2}$$

ist, so leuchtet die Richtigkeit des Satzes ein.

6. Ist P eine ungerade Zahl, so ist

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

Denn mit Beibehaltung derselben Zeichen ist

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p'}\right)\left(\frac{2}{p''}\right)\left(\frac{2}{p'''}\right)\cdots = (-1)^{\Sigma\frac{p^2-1}{8}},$$

und da nach dem zweiten Lemma 4.

$$\Sigma \frac{p^2-1}{8} \equiv \frac{P^2-1}{8} \pmod{2}$$

ist, so ergiebt sich unmittelbar die Richtigkeit des zu beweisenden Satzes.

7. Sind die beiden positiven ungeraden Zahlen P und Q relative Primzahlen zu einander, so ist

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Denn es sei P das Product aus den Primzahlen

$$p', p'', p''' \ldots \qquad (p)$$

und Q das Product aus den Primzahlen

$$q', q'' \ldots \qquad (q)$$

welche also von den Primzahlen $p', p'', p''' \ldots$ verschieden sind. Dann ist zufolge der Erklärung und nach 2.

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q'}\right)\left(\frac{P}{q''}\right)\cdots = \Pi\left(\frac{p}{q}\right),$$

wo das Productzeichen Π sich auf alle Combinationen einer jeden der Primzahlen p mit einer jeden der Primzahlen q bezieht; ganz ebenso ist aber

$$\left(\frac{Q}{P}\right) = \Pi\left(\frac{q}{p}\right)$$

und folglich

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \Pi\left(\frac{p}{q}\right)\left(\frac{q}{p}\right),$$

wo das Productzeichen sich auf dieselben Combinationen bezieht; da nun nach dem Reciprocitätssatze

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ist, so ergiebt sich

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\Sigma\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

wo wieder das Summenzeichen sich auf dieselben Combinationen jeder Primzahl p mit jeder Primzahl q erstreckt; es ist daher

$$\Sigma\frac{p-1}{2}\frac{q-1}{2}=\Sigma\frac{p-1}{2}\times\Sigma\frac{q-1}{2},$$

wo auf der rechten Seite das erste Summenzeichen sich auf alle Primzahlen p, das zweite sich auf alle Primzahlen q bezieht. Da nun nach dem ersten Lemma 4.

$$\Sigma\frac{p-1}{2}\equiv\frac{P-1}{2}\pmod{2}$$

und

$$\Sigma\frac{q-1}{2}\equiv\frac{Q-1}{2}\pmod{2}$$

ist, so ergiebt sich

$$\Sigma\frac{p-1}{2}\frac{q-1}{2}\equiv\frac{P-1}{2}\frac{Q-1}{2}\pmod{2},$$

und hieraus

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}},$$

was zu beweisen war. —

Es bleibt uns nun noch eine Bemerkung über das Symbol zu machen übrig; wir haben oben dieses Zeichen nur unter der Voraussetzung definirt, dass die Zahl P eine *positive ungerade* Zahl, und dass die positive oder negative Zahl m *relative Primzahl zu* P ist; wir erweitern jetzt die Bedeutung des Zeichens dahin, dass P auch eine *negative ungerade* Zahl sein kann, immer aber mit der Beschränkung, dass m *relative Primzahl zu* P ist*); und zwar setzen wir fest, dass

$$\left(\frac{m}{-P}\right)=\left(\frac{m}{P}\right)$$

---

*) Später (Supplemente §. 116) werden wir festsetzen, dass das Symbol den Werth *Null* haben soll, sobald P eine ungerade Zahl, m aber keine relative Primzahl zu P ist.

sein soll. Dann leuchtet augenblicklich ein, dass die Sätze 1., 2., 3. und 6. ohne Beschränkung gültig bleiben; ferner, dass der Satz 5. nur dann richtig ist, wenn P positiv ist, dagegen für ein negatives P falsch wird; und endlich, dass der Satz 7. nur dann gültig bleibt, wenn mindestens eine der beiden Zahlen P und Q positiv ist, dagegen seine Gültigkeit verliert, wenn beide Zahlen P und Q negativ sind.

§. 47.

Die oben (§. 45) an einem Beispiel behandelte Aufgabe, den Werth des Legendre'schen Symbols zu bestimmen, bildet offenbar nur einen ganz speciellen Fall der allgemeinen Aufgabe, den Werth des Jacobi'schen Symbols zu bestimmen. Es zeigt sich nun, dass die damals nothwendige Zerlegung in Primzahlfactoren (abgesehen von dem Factor 2) ganz überflüssig geworden, und der anzuwendende Algorithmus demjenigen ganz ähnlich ist, durch welchen der grösste gemeinschaftliche Divisor zweier Zahlen gefunden wird. Einige Beispiele werden genügen, um diese einfachere Methode zu erläutern.

Beispiel 1: Nehmen wir das schon oben (§. 45) behandelte Beispiel, so können wir jetzt nach dem verallgemeinerten Reciprocitätssatze

$$\left(\frac{365}{1847}\right) = \left(\frac{1847}{365}\right)$$

setzen, weil 365 von der Form $4n+1$ ist. Da ferner $1847 \equiv 22$ (mod. 365) ist, so ist nach §. 46, 3. und 2.

$$\left(\frac{1847}{365}\right) = \left(\frac{22}{365}\right) = \left(\frac{2}{365}\right)\left(\frac{11}{365}\right);$$

da ferner $365 \equiv 5$ (mod. 8), so ist nach §. 46, 6.

$$\left(\frac{2}{365}\right) = -1,$$

also

$$\left(\frac{365}{1847}\right) = -\left(\frac{11}{365}\right).$$

Nach dem verallgemeinerten Reciprocitätssatz ist nun wieder

$$\left(\frac{365}{11}\right) = \left(\frac{365}{11}\right) = \left(\frac{2}{11}\right) = -1,$$

und folglich

$$\left(\frac{365}{1847}\right) = +1,$$

wie früher.

Beispiel 2: Nach dem verallgemeinerten Reciprocitätssatze ist

$$\left(\frac{195}{1901}\right) = \left(\frac{1901}{195}\right);$$

weil $1901 \equiv -49 \pmod{195}$, so ist

$$\left(\frac{1901}{195}\right) = \left(\frac{-49}{195}\right);$$

da ferner die Zahlen -49 und 195 nicht beide negativ sind, so gilt für sie der verallgemeinerte Reciprocitätssatz, und, weil beide von der Form $4n+3$ sind, so ist

$$\left(\frac{-49}{195}\right) = -\left(\frac{195}{-49}\right) = -\left(\frac{195}{49}\right);$$

weil endlich $195 \equiv -1 \pmod{49}$, und 49 von der Form $4n+1$ ist, so ist

$$\left(\frac{195}{49}\right) = \left(\frac{-1}{49}\right) = +1,$$

also

$$\left(\frac{195}{1901}\right) = -1$$

d. h. 195 ist quadratischer Nichtrest der Primzahl 1901. Natürlich hätte sich die Auflösung abkürzen lassen durch Zerlegung in Factoren, nämlich durch die Bemerkung, dass $49 = 7 \,.\, 7$ und folglich

$$\left(\frac{-49}{195}\right) = \left(\frac{-1}{195}\right) = -1$$

ist; überhaupt wird die Operation immer bedeutend abgekürzt, wenn man im Zähler oder Nenner des Symbols quadratische Factoren bemerkt, da diese sogleich fortgelassen werden können.

Beispiel 3: Da $74 = 2 \,.\, 37$, und $101 \equiv 5 \pmod{8}$ ist, so ist

$$\left(\frac{74}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{37}{101}\right) = -\left(\frac{37}{101}\right);$$

dann ist ferner nach dem Reciprocitätssatze

$$\left(\frac{37}{101}\right) = \left(\frac{101}{37}\right) = \left(\frac{-10}{37}\right) = \left(\frac{10}{37}\right)$$

und, weil 37 von der Form $8n + 5$ ist,

$$\left(\frac{10}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = -\left(\frac{5}{37}\right);$$

endlich ist wieder nach dem Reciprocitätssatze

$$\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1$$

und folglich

$$\left(\frac{74}{101}\right) = -1.$$

Kürzer gelangt man durch folgende Kette zum Ziele:

$$\left(\frac{74}{101}\right) = \left(\frac{-27}{101}\right) = \left(\frac{101}{-27}\right) = \left(\frac{-7}{27}\right) = \left(\frac{27}{-7}\right) = \left(\frac{-1}{7}\right)$$
$$= -1.$$

§. 48.

Wegen der Wichtigkeit des Reciprocitätssatzes theilen wir hier noch einen andern Beweis desselben mit, nämlich den *ersten* der von *Gauss* gegebenen sechs Beweise*); dies kann hier um so eher geschehen, als durch die im Vorhergehenden erörterte Verallgemeinerung des Legendre'schen Symbols mehrere der von *Gauss* unterschiedenen acht Fälle sich zusammenziehen lassen, wodurch der Beweis an Kürze und Uebersichtlichkeit bedeutend gewinnt**).

Das Wesen dieses Beweises besteht in der sogenannten vollständigen Induction; wenn nämlich der Satz für je zwei Primzahlen p, p' richig ist, welche kleiner sind, als eine bestimmte Primzahl q, so lässt sich zeigen, dass er auch für jede Combination einer solchen Primzahl p mit der Primzahl q selbst gelten muss; hieraus und weil der Satz für die beiden kleinsten ungeraden

*) *Disquisitiones Arithmeticae* artt. 135—144.

**) *Dirichlet: Ueber den ersten der von Gauss gegebenen Beweise des Reciprocitätsgesetzes in der Theorie der quadratischen Reste* (Crelle's Journal XLVII).

Primzahlen 3 und 5 wirklich richtig ist, folgt dann unmittelbar seine Allgemeingültigkeit

Von besonderer Wichtigkeit für diesen Nachweis ist nun die vorläufige Bemerkung, dass aus der angenommenen Richtigkeit des Reciprocitätssatzes für je zwei Primzahlen p, p', welche kleiner als die Primzahl q sind, mit Nothwendigkeit auch die Gültigkeit des verallgemeinerten Satzes (§. 46, 7.)

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$$

folgt, sobald die beiden ungeraden relativen Primzahlen P und Q (die nicht gleichzeitig negativ sein dürfen) nur solche Primzahlfactoren enthalten, die kleiner als q sind; denn der Beweis dieses verallgemeinerten Satzes gründete sich ausschliesslich auf die Richtigkeit des einfachen Satzes für alle die Paare von zwei Primzahlen, von denen die eine in P, die andere in Q aufgeht.

Bei dem Beweise nun, dass der Reciprocitätssatz für jede Combination von q mit einer Primzahl p gilt, welche kleiner als q ist, haben wir zwei Fälle zu unterscheiden. Der eine Fall und zwar der schwierigere findet Statt, wenn q die Form $4n+1$ hat, und zugleich p quadratischer Nichtrest von q ist; dann ist zu beweisen, dass auch q quadratischer Nichtrest von p ist. In irgend einem der andern Fälle, nämlich wenn q von der Form $4n+3$ ist, oder auch, wenn q zwar die Form $4n+1$ hat, dann aber p quadratischer Rest von q ist, kann man offenbar der Primzahl p immer ein solches Vorzeichen geben, dass, wenn man $\omega = \pm p$ setzt, wenigstens für eins der beiden Vorzeichen ω quadratischer Rest von q wird; dann ist also zu beweisen, dass

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1) \cdot \frac{1}{2}(q-1)}$$

ist; dieser letztere Fall ist deshalb leichter zu behandeln, weil die Annahme sogleich einen Ansatz giebt, welcher nur ausgebeutet zu werden braucht. Wir beginnen daher mit diesem Theile des Satzes.

§. 49.

Es sei also $\omega = \pm p$ quadratischer Rest von q, so hat die Congruenz $x^2 \equiv \omega \pmod{q}$ zwischen 0 und q immer zwei Wurzeln x

deren Summe $= q$, und von denen folglich die eine, welche wir mit e bezeichnen wollen, eine gerade Zahl ist. Dann wird

$$e^2 - \omega = qf$$

sein, wo f eine ganze Zahl bedeutet, welche jedenfalls nicht $= 0$ ist, weil sonst die Primzahl ω eine Quadratzahl sein müsste. Diese Zahl f kann aber auch nicht negativ sein; denn sonst wäre ω positiv $= p$, und $p - e^2$ eine positive durch q theilbare Zahl, was aber unmöglich ist, da $p - e^2 < p$, und der Voraussetzung nach $p < q$ ist. Diese positive Zahl f muss ferner ungerade sein; denn da e gerade ist, so ist $e^2 - \omega$ ungerade, und folglich auch jeder Divisor von $e^2 - \omega$, also auch f ungerade. Endlich ist diese positive ungerade Zahl f nothwendig $< q - 1$; denn da $e \leqq q - 1$, und $p < q - 1$, so ist $qf = e^2 - \omega < (q-1)^2 + (q-1)$, d. h. $qf < q(q-1)$, also wirklich $f < q - 1$.

Nun sind zwei Fälle möglich:

1. Ist f nicht durch p theilbar, so folgt aus der Gleichung $e^2 - \omega = qf$, dass

$$\left(\frac{\omega}{f}\right) = +1,$$

und ferner, weil qf quadratischer Rest von p ist, dass

$$\left(\frac{q}{\omega}\right) = \left(\frac{f}{\omega}\right)$$

sein muss; da nun die beiden ungeraden Zahlen f und ω relative Primzahlen zu einander, beide kleiner als q, und endlich nicht beide negativ sind, so gilt für sie der verallgemeinerte Reciprocitätssatz, d. h. es ist

$$\left(\frac{f}{\omega}\right)\left(\frac{\omega}{f}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(f-1)}$$

und hieraus ergiebt sich unter Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(f-1)}.$$

Da ferner e eine gerade Zahl ist, so ist auch $-\omega \equiv qf \pmod{4}$, also (nach dem ersten Lemma 4. in §. 46)

$$-\frac{\omega+1}{2} \equiv \frac{qf-1}{2} \equiv \frac{q-1}{2} + \frac{f-1}{2} \pmod{2};$$

multiplicirt man diese Congruenz mit $\frac{1}{2}(\omega - 1)$, so erhält man auf

der linken Seite ein Product aus zwei successiven ganzen Zahlen, also gewiss eine gerade Zahl, und hieraus folgt unmittelbar

$$\frac{\omega-1}{2}\,\frac{f-1}{2} \equiv \frac{\omega-1}{2}\,\frac{q-1}{2} \pmod{2}$$

und also

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(q-1)},$$

was zu beweisen war.

2. Ist dagegen f theilbar durch p, so kann man $f = \omega\varphi$ setzen, wo φ eine ungerade Zahl bedeutet, die dasselbe Zeichen wie ω hat und ihrem absoluten Werthe nach $< q$ ist. Da nun $e^2 - \omega = q\omega\varphi$, so ist auch e theilbar durch ω und also $e = \varepsilon\omega$, wo ε wieder eine gerade Zahl ist. Hieraus ergiebt sich nun

$$\varepsilon^2\omega - 1 = q\varphi,$$

und es kann daher φ nicht durch ω theilbar sein. Nun war ω quadratischer Rest von $f = \omega\varphi$, und folglich auch von φ, also ist

$$\left(\frac{\omega}{\varphi}\right) = \left(\frac{\omega}{-\varphi}\right) = +1;$$

ausserdem folgt aus der vorhergehenden Gleichung, dass $-q\varphi$ quadratischer Rest von ω, dass also

$$\left(\frac{q}{\omega}\right) = \left(\frac{-\varphi}{\omega}\right)$$

ist; da endlich von den beiden ungeraden Zahlen $-\varphi$ und ω die eine positiv ist, und da sie relative Primzahlen zu einander und ausserdem beide $< q$ sind, so ist nach dem verallgemeinerten Reciprocitätssatze

$$\left(\frac{-\varphi}{\omega}\right)\left(\frac{\omega}{-\varphi}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(\varphi+1)}$$

und folglich unter Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(\varphi+1)}.$$

Da nun ε eine gerade Zahl und folglich $q\varphi \equiv -1 \pmod{4}$ ist, so muss die eine der beiden Zahlen φ und q von der Form $4n+1$, die andere aber von der Form $4n+3$ sein, woraus folgt, dass

$$\frac{\varphi+1}{2} \equiv \frac{q-1}{2} \pmod{2}$$

und also

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1) \cdot \frac{1}{2}(q-1)}$$

ist. Also ist auch für diesen Fall der Satz bewiesen.

§. 50.

Wir kommen nun zu dem zweiten Theile, in welchem vorausgesetzt wird, dass p Nichtrest von q, und q von der Form $4n+1$ ist, und in welchem bewiesen werden muss, dass q Nichtrest von p ist. Hier fehlt nun die Möglichkeit eines Ansatzes, und um diese zu gewinnen, kommt alles darauf an nachzuweisen, dass wenigstens eine Primzahl $p' < q$ existirt, von welcher q quadratischer Nichtrest ist, oder mit anderen Worten, dass die Primzahl q nicht von allen kleineren Primzahlen quadratischer Rest sein kann. Für den Fall, dass $q \equiv 5 \pmod{8}$ ist, hat dieser Nachweis nicht die geringste Schwierigkeit; denn dann ist $\frac{1}{2}(q+1) \equiv 3 \pmod{4}$, und folglich muss unter den Primfactoren dieser Zahl $\frac{1}{2}(q+1)$, welche natürlich alle $< q$ sind, mindestens einer p' von der Form $4n+3$ sein; dann ist aber $q \equiv -1 \pmod{p'}$ und folglich quadratischer Nichtrest einer kleinern Primzahl p'. Desto schwieriger war dieser Nachweis für den andern Fall zu führen, in welchem $q \equiv 1 \pmod{8}$ ist; und *Gauss* selbst gesteht*), dass es ihm erst nach manchen vergeblichen Versuchen gelungen ist, diese capitale Schwierigkeit zu überwinden; er gelangte dazu durch folgende äusserst scharfsinnige Betrachtung.

Es sei $2m+1$ irgend eine ungerade Zahl, aber kleiner als q. Wenn nun q quadratischer Rest von allen ungeraden Primzahlen z ist, welche diese ungerade Zahl $2m+1$ nicht übertreffen, so ist nach früheren Sätzen (§. 37) die Primzahl q, da sie $\equiv 1 \pmod{8}$ und also von jeder Potenz der Zahl 2 quadratischer Rest ist, auch quadratischer Rest von jeder Zahl, welche keine anderen ungeraden Primfactoren als die Primzahlen z enthält, und also z. B. von der Zahl

*) *D. A.* art. 125.

$$M = 1 . 2 . 3 . 4 \ldots\ldots (2m)(2m+1);$$

es giebt daher positive Zahlen k von der Beschaffenheit, dass

$$q \equiv k^2 \pmod{M}$$

ist, und zwar muss k relative Primzahl zu M sein, weil $2m+1<q$ und also auch q relative Primzahl zu M ist. Aus dieser Congruenz folgt nun weiter, dass in Bezug auf den Modul M

$$k(q-1^2)(q-2^2)(q-3^2)\ldots(q-m^2)$$
$$\equiv k(k^2-1^2)(k^2-2^2)(k^2-3^2)\ldots(k^2-m^2)$$
$$\equiv (k+m)(k+m-1)\ldots(k+1)\,k(k-1)\ldots(k-m+1)(k-m)$$

ist; da nun nach einem frühern Satze (§. 15) jedes Product von $(2m+1)$ successiven ganzen Zahlen durch M theilbar, und ausserdem k relative Primzahl zu M ist, so ist das Product

$$(q-1^2)(q-2^2)(q-3^2)\ldots(q-m^2)$$

theilbar durch das Product

$$M = (m+1)((m+1)^2-1^2)((m+1)^2-2^2)\ldots((m+1)^2-m^2)$$

d. h. das Product

$$\frac{1}{m+1}\cdot\frac{q-1^2}{(m+1)^2-1^2}\cdot\frac{q-2^2}{(m+1)^2-2^2}\cdots\frac{q-m^2}{(m+1)^2-m^2}$$

ist nothwendig eine ganze Zahl.

Andererseits leuchtet ein, dass dies Product gewiss keine ganze Zahl ist, sobald für m die grösste ganze Zahl unterhalb $\sqrt{q}$ genommen wird; denn, wenn $m<\sqrt{q}<m+1$ ist, so sind alle Factoren dieses Productes echte Brüche. Da nun ausserdem $2m+1<2\sqrt{q}+1<q$ ist, so kann für diese Zahl m die Annahme nicht zulässig sein, und wir haben daher folgenden Satz gewonnen:

Ist q eine Primzahl von der Form $8n+1$, so giebt es unterhalb $2\sqrt{q}+1$ und folglich auch unterhalb q mindestens eine ungerade Primzahl p', von welcher q quadratischer Nichtrest ist.

§. 51.

Nachdem für jede Primzahl q von der Form $4n+1$ die Existenz einer Primzahl $p'<q$ nachgewiesen ist, von welcher q quadratischer Nichtrest ist, gehen wir zum Beweise unseres zweiten Theiles über. Jede solche Primzahl p' muss Nichtrest von q sein;

denn wäre p' Rest von q, so würde aus dem schon von uns bewiesenen Theil (§. 49)

$$\left(\frac{q}{p'}\right) = (-1)^{\frac{1}{2}(p'-1) \cdot \frac{1}{2}(q-1)} = +1$$

folgen, was mit der Voraussetzung streitet. Mithin gilt für diese Primzahl p' das Reciprocitätsgesetz. Giebt es nun *ausser* p' noch *andere* ungerade Primzahlen $p < q$, welche Nichtreste von q sind, so ist nur zu beweisen, dass

$$\left(\frac{q}{pp'}\right) = +1$$

ist, weil hieraus sogleich folgt, dass q Nichtrest von p ist. Da nun der Voraussetzung nach p' und p quadratische Nichtreste von q sind, so ist pp' quadratischer Rest von q, und es giebt daher wieder eine gerade Zahl $e < q$ von der Beschaffenheit, dass

$$e^2 - pp' = q\varphi$$

und φ eine ganze Zahl ist; und weil die linke Seite dieser Gleichung eine ungerade Zahl darstellt, welche ihrem absoluten Werthe nach $< q^2$ ist, so ist φ ebenfalls eine ungerade Zahl und zwar $< q$. Je nach der Beschaffenheit dieser Zahl φ zerfällt nun der Beweis in drei Theile.

1. Ist φ weder durch p noch durch p' theilbar, so ist

$$\left(\frac{pp'}{\varphi}\right) = +1,$$

und da $q\varphi$ quadratischer Rest von pp' ist, auch

$$\left(\frac{q\varphi}{pp'}\right) = 1, \text{ also } \left(\frac{q}{pp'}\right) = \left(\frac{\varphi}{pp'}\right);$$

da ferner die beiden ungeraden relativen Primzahlen φ und pp' (von denen die letztere positiv ist) nur solche Primfactoren enthalten, welche $< q$ sind, so gilt für diese beiden Zahlen auch das verallgemeinerte Reciprocitätsgesetz, d. h. es ist

$$\left(\frac{\varphi}{pp'}\right)\left(\frac{pp'}{\varphi}\right) = (-1)^{\frac{1}{2}(\varphi-1) \cdot \frac{1}{2}(pp'-1)}$$

und folglich, mit Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(\varphi-1) \cdot \frac{1}{2}(pp'-1)}.$$

Da aber e eine gerade Zahl, so ist $q\varphi \equiv -pp'$ (mod. 4), also, da $q \equiv 1$ (mod. 4) ist,

$$\varphi \equiv -pp' \pmod{4}$$

$$\frac{\varphi - 1}{2} \equiv -\frac{pp' + 1}{2} \pmod{2}$$

also

$$\frac{\varphi - 1}{2} \cdot \frac{pp' - 1}{2} \equiv 0 \pmod{2}$$

und folglich

$$\left(\frac{q}{pp'}\right) = 1,$$

was zu beweisen war.

2. Ist φ durch p' theilbar, durch p nicht theilbar, so setze man $\varphi = p'\psi$, und, da auch e durch p' theilbar sein muss, $e = p'\varepsilon$; dann ist $\psi < q$ eine durch p nicht theilbare ungerade, und ε eine gerade Zahl, und es wird

$$p'\varepsilon^2 - p = q\psi.$$

Hieraus folgt nun zunächst wieder (da ψ relative Primzahl zu pp' ist)

$$\left(\frac{pp'}{\psi}\right) = +1,$$

ferner

$$\left(\frac{q\psi}{p}\right) = \left(\frac{p'}{p}\right), \quad \text{also} \quad \left(\frac{q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{\psi}{p}\right)$$

und

$$\left(\frac{q\psi}{p'}\right) = \left(\frac{-p}{p'}\right), \quad \text{also} \quad \left(\frac{q}{p'}\right) = \left(\frac{-p}{p'}\right)\left(\frac{\psi}{p'}\right)$$

und folglich

$$\left(\frac{q}{pp'}\right) = \left(\frac{p'}{-p}\right)\left(\frac{-p}{p'}\right)\left(\frac{\psi}{pp'}\right) = (-1)^{\frac{1}{2}(p+1) \cdot \frac{1}{2}(p'-1)}\left(\frac{\psi}{pp'}\right);$$

da endlich ψ und pp' nur solche Primfactoren enthalten, die $< q$ sind, so ist nach dem verallgemeinerten Reciprocitätssatz

$$\left(\frac{\psi}{pp'}\right)\left(\frac{pp'}{\psi}\right) = (-1)^{\frac{1}{2}(\psi-1) \cdot \frac{1}{2}(pp'-1)}$$

und hieraus in Verbindung mit zwei vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(p+1) \cdot \frac{1}{2}(p'-1) + \frac{1}{2}(\psi-1) \cdot \frac{1}{2}(pp'-1)}.$$

Da nun $\varepsilon^2 \equiv 0 \pmod{4}$ und $q \equiv 1 \pmod{4}$, so ist $\psi \equiv -p \pmod{4}$, folglich

$$\tfrac{1}{2}(\psi - 1) \equiv \tfrac{1}{2}(p + 1) \pmod{2},$$

also

$$\tfrac{1}{2}(p+1).\tfrac{1}{2}(p'-1)+\tfrac{1}{2}(\psi-1).\tfrac{1}{2}(pp'-1)$$
$$\equiv \tfrac{1}{2}(p+1)\,[\tfrac{1}{2}(p'-1)+\tfrac{1}{2}(pp'-1)] \pmod{2},$$

und da ferner (nach dem ersten Lemma 4. in §. 46)

$$\tfrac{1}{2}(pp'-1)\equiv\tfrac{1}{2}(p-1)+\tfrac{1}{2}(p'-1) \pmod{2}$$

ist, so ergiebt sich

$$\tfrac{1}{2}(p+1).\tfrac{1}{2}(p'-1)+\tfrac{1}{2}(\psi-1).\tfrac{1}{2}(pp'-1)$$
$$\equiv\tfrac{1}{2}(p+1).\tfrac{1}{2}(p-1)\equiv 0 \pmod{2}$$

und folglich

$$\left(\frac{q}{pp'}\right)=1,$$

was zu beweisen war.

Da bei diesem Beweise die Annahme, dass q Nichtrest von p' ist, gar nicht zur Anwendung gekommen ist, so wird durch einfache Vertauschung von p mit p' der Beweis für den Fall entstehen, dass φ durch p theilbar, durch p' nicht theilbar ist; denn im Uebrigen sind sowohl die Voraussetzungen als auch das zu beweisende Resultat vollständig symmetrisch in Bezug auf beide Primzahlen p und p'.

3. Ist φ sowohl durch p als auch durch p' und folglich (da p und p' verschiedene Primzahlen sind) auch durch pp' theilbar, so setze man $\varphi = pp'\psi$, und, da e dann ebenfalls durch pp' theilbar ist, $e = pp'\varepsilon$; dann bedeutet ψ eine ungerade Zahl $< q$, und ε eine gerade Zahl, und es wird

$$pp'\varepsilon^2-1=q\psi.$$

Hieraus folgt, dass pp' relative Primzahl zu ψ und ausserdem quadratischer Rest von ψ, also

$$\left(\frac{pp'}{\psi}\right)=+1$$

ist; ebenso ergiebt sich aber, dass $-q\psi$ quadratischer Rest von pp', dass also

$$\left(\frac{q}{pp'}\right)=\left(\frac{-\psi}{pp'}\right)$$

ist; nach dem verallgemeinerten Reciprocitätssatze, welcher offenbar für die beiden Zahlen $-\psi$ und pp' gilt, ist ferner

$$\left(\frac{-\psi}{pp'}\right)\left(\frac{pp'}{-\psi}\right)=(-1)^{\frac{1}{2}(pp'-1).\frac{1}{2}(\psi+1)},$$

und hieraus ergiebt sich in Verbindung mit den beiden vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(pp'-1)\cdot\frac{1}{2}(\psi+1)}.$$

Da aber ε eine gerade Zahl, und $q \equiv 1$ (mod. 4), so ist $\psi \equiv -1$ (mod. 4), also $\frac{1}{2}(\psi + 1)$ eine gerade Zahl, und folglich

$$\left(\frac{q}{pp'}\right) = 1,$$

was zu beweisen war.

Hiermit ist nun auch der zweite Theil des Beweises vollständig geführt und dadurch die Allgemeingültigkeit des Reciprocitätssatzes von Neuem nachgewiesen (ein dritter Beweis findet sich in den Supplementen I. §. 115). Auf ähnliche Weise lassen sich auch die Sätze über die Charaktere der Zahlen -1 und 2 begründen, was dem Leser überlassen bleiben mag*).

§. 52.

Nach allen diesen Untersuchungen kehren wir nun zurück zu der Beantwortung der zweiten in §. 32 aufgeworfenen Frage, welche in §. 39 auf die folgende reducirt ist:

Von welchen ungeraden Primzahlen q ist die gegebene Zahl D quadratischer Rest?

Auch jetzt fragen wir nur nach denjenigen (positiv genommenen) Primzahlen q, welche nicht in D aufgehen, und setzen ausserdem der Einfachheit halber voraus, dass D kein Quadrat und auch durch kein Quadrat (ausser 1) theilbar ist, weil der allgemeinere Fall offenbar sogleich auf diesen einfachern reducirt werden kann. Es wird sich zeigen, dass nicht blos alle diese Primzahlen q (die *Divisoren der Form* $t^2 - Du^2$ nach §. 39), sondern überhaupt alle positiven Zahlen n, welche relative Primzahlen zu $2D$ sind und der Bedingung

$$\left(\frac{D}{n}\right) = +1$$

*) *Dirichlet* a. a. O.

genügen, in einer Anzahl von bestimmten Linearformen, d. h. von arithmetischen Reihen enthalten sind, deren Differenz entweder $= 2D$ oder $= 4D$ ist. Da wir vorausgesetzt haben, dass die positive oder negative Zahl D durch keine Quadratzahl theilbar ist, so wird, wenn wir das Product aller in D aufgehenden positiven ungeraden Primzahlen $p, p', p'' \ldots$ mit P bezeichnen, entweder $D = \pm P$, oder $D = \pm 2P$ sein; wenn D keine ungerade Primzahl p als Factor enthält (für welchen Fall das Resultat aber schon in den §§. 40, 41 oder allgemeiner in §. 46, 5. und 6. angegeben ist), wird $P = 1$ zu setzen sein. Wir unterscheiden im Ganzen vier Fälle.

I. $D = \pm P \equiv 1 \pmod{4}$.

In diesem Falle ist, wenn n irgend eine *positive* Zahl bedeutet, die relative Primzahl zu $2D$ ist, zufolge des verallgemeinerten Reciprocitätssatzes (§. 46, 7.)

$$\left(\frac{D}{n}\right) = \left(\frac{n}{P}\right).$$

Da nun das Symbol rechts für alle Zahlen n, welche einer und derselben Classe (mod. P) angehören, nach §. 46, 3. einen und denselben Werth besitzt, so kommt es offenbar nur darauf an, ein vollständiges System von $\varphi(P)$ incongruenten Zahlen m (mod. P) zu betrachten, die relative Primzahlen zu P sind, und für jede den Werth des Symbols zu bestimmen. Es ist wichtig, dies etwas näher zu untersuchen.

Zunächst lässt sich beweisen, dass Zahlen b existiren, welche der Bedingung

$$\left(\frac{b}{P}\right) = -1 \tag{1}$$

genügen. Denn da D nicht $= +1$ sein kann, und folglich P mindestens eine Primzahl p enthält, so wähle man einen beliebigen Nichtrest β von p, und bestimme b (nach §. 25) durch die Bedingungen

$$b \equiv \beta \pmod{p}, \quad b \equiv 1 \pmod{P'},$$

wo $P = pP'$ gesetzt ist, so wird

$$\left(\frac{b}{P}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{P'}\right) = \left(\frac{\beta}{p}\right)\left(\frac{1}{P'}\right) = -1.$$

Nachdem dieser Punct absolvirt ist, erkennt man leicht, dass die Anzahl aller incongruenten Zahlen b (mod. P), welche der Be-

dingung (1) genügen, $= \frac{1}{2}\varphi(P)$, und folglich die Anzahl aller incongruenten Zahlen a (mod. P), für welche

$$\left(\frac{a}{P}\right) = +1 \tag{2}$$

ist, ebenso gross ist. Denn setzt man

$$S = \Sigma \left(\frac{m}{P}\right),$$

wo m das ganze System aller $\varphi(P)$ incongruenten Zahlen durchlaufen soll, so ist S gänzlich unabhängig von der Wahl der die einzelnen Zahlclassen repräsentirenden Individuen m; da nun, wenn b eine bestimmte Zahl von der Beschaffenheit (1) bedeutet, auch die Producte bm ein solches vollständiges System bilden, so ist auch

$$S = \Sigma \left(\frac{bm}{P}\right) = \left(\frac{b}{P}\right) \Sigma \left(\frac{m}{P}\right) = -S$$

und folglich

$$\Sigma \left(\frac{m}{P}\right) = 0, \tag{3}$$

mithin ist die Anzahl der Glieder dieser Summe, welche den Werth $+1$ haben, gleich der Anzahl derjenigen, welche den Werth -1 haben; d. h. die Anzahl der Zahlclassen a ist gleich derjenigen der Zahlclassen b.

Es leuchtet ferner ein, dass man die Repräsentanten m (oder a und b) sämmtlich *ungerade* wählen kann; denn ist m gerade, so ist $m + P$ eine in derselben Zahlclasse enthaltene ungerade Zahl. Dann wird also

$$\left(\frac{D}{n}\right) = +1, \quad \text{wenn} \quad n \equiv a \ (\text{mod. } 2P)$$

$$\left(\frac{D}{n}\right) = -1, \quad \text{wenn} \quad n \equiv b \ (\text{mod. } 2P)$$

und jede (positive) Zahl n, welche relative Primzahl zu $2D$ ist, ist in einer und nur einer dieser arithmetischen Reihen (von der Differenz $2D$) enthalten.

Beispiel 1. Ist $D = +P = 21$, also $\varphi(P) = 12$, so sind die sämmtlichen relativen Primzahlen zu P congruent

$$\pm 1, \pm 2, \pm 4, \pm 5, \pm 8, \pm 10;$$

bestimmt man nun für jede dieser Zahlen den Werth des Jacobi'schen Symbols nach §. 47, so ergiebt sich

$$a \equiv \pm 1, \pm 4, \pm 5; \quad b \equiv \pm 2, \pm 8, \pm 10;$$

es wird daher

$$\left(\frac{21}{n}\right) = +1, \quad \text{wenn} \quad n \equiv 1, 5, 17, 25, 37, 41 \pmod{42}$$

$$\left(\frac{21}{n}\right) = -1, \quad \text{wenn} \quad n \equiv 11, 13, 19, 23, 29, 31 \pmod{42}.$$

Beispiel 2. Ist $D = -P = -15$, so sind die zu betrachtenden Zahlenclassen folgende $\pm 1, \pm 2, \pm 4, \pm 7$; diese zerfallen in $a \equiv +1, +2, +4, -7$, und $b \equiv -1, -2, -4, +7$. Es wird daher

$$\left(\frac{-15}{n}\right) = +1, \quad \text{wenn} \quad n \equiv 1, 17, 19, 23 \pmod{30}$$

$$\left(\frac{-15}{n}\right) = -1, \quad \text{wenn} \quad n \equiv 7, 11, 13, 29 \pmod{30}.$$

Wir gehen nun über zu dem Fall

II. $D = \pm P \equiv 3 \pmod{4}$.

Bedeutet n wieder eine *positive* relative Primzahl zu $2D$, so ist nach dem allgemeinen Reciprocitätssatz

$$\left(\frac{D}{n}\right) = (-1)^{\frac{n-1}{2}} \left(\frac{n}{P}\right);$$

behalten wir dieselbe Bezeichnung wie im ersten Falle bei, so wird

$$\left(\frac{D}{n}\right) = +1, \quad \text{wenn} \quad n \equiv 1 \pmod{4} \quad \text{und} \quad n \equiv a \pmod{P}$$
$$\text{oder} \quad n \equiv 3 \pmod{4} \quad \text{und} \quad n \equiv b \pmod{P}$$

dagegen

$$\left(\frac{D}{n}\right) = -1, \quad \text{wenn} \quad n \equiv 1 \pmod{4} \quad \text{und} \quad n \equiv b \pmod{P}$$
$$\text{oder} \quad n \equiv 3 \pmod{4} \quad \text{und} \quad n \equiv a \pmod{P}.$$

Einem jeden solchen Congruenzpaare entspricht aber (nach §. 25) eine bestimmte Classe von Zahlen n (mod. $4P$); man erhält daher $\varphi(P) = \frac{1}{2}\varphi(4P)$ solche Classen von Zahlen n, die der einen Kategorie angehören, und ebenso viele Classen von Zahlen n, die den entgegengesetzten Charakter haben; diese Classen bilden arithmetische Reihen von der Differenz $4D$. Dies Resultat gilt auch noch in dem Falle $D = -1$, obgleich dann keine Zahl b existirt.

Beispiel. Für $D = +15$ wird

$\left(\frac{D}{n}\right) = +1$, wenn $n \equiv 1 \pmod{4}$, $\equiv +1, +2, +4, -7 \pmod{15}$
oder $n \equiv 3 \pmod{4}$, $\equiv -1, -2, -4, +7 \pmod{15}$

dagegen

$\left(\frac{D}{n}\right) = -1$, wenn $n \equiv 1 \pmod{4}$, $\equiv -1, -2, -4, +7 \pmod{15}$
oder $n \equiv 3 \pmod{4}$, $\equiv +1, +2, +4, -7 \pmod{15}$;

hieraus ergiebt sich

$\left(\frac{15}{n}\right) = +1$, wenn $n \equiv 1, 7, 11, 17, 43, 49, 53, 59 \pmod{60}$

$\left(\frac{15}{n}\right) = -1$, wenn $n \equiv 13, 19, 23, 29, 31, 37, 41, 47 \pmod{60}$.

Die Rechnung gestaltet sich am einfachsten, wenn man die sämmtlichen positiven relativen Primzahlen zu $4P$ darauf prüft, ob sie der einen oder andern Kategorie angehören, und sie lässt sich noch durch manche Kunstgriffe abkürzen, die hier nicht erwähnt werden können.

III. $D = \pm 2P \equiv 2 \pmod{8}$.

In diesem Falle ist, wenn n eine *positive* relative Primzahl zu D bedeutet,

$$\left(\frac{D}{n}\right) = (-1)^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right),$$

und folglich

$\left(\frac{D}{n}\right) = +1$, wenn $n \equiv \pm 1 \pmod{8}$, $\equiv a \pmod{P}$
oder $n \equiv \pm 3 \pmod{8}$, $\equiv b \pmod{P}$

dagegen

$\left(\frac{D}{n}\right) = -1$, wenn $n \equiv \pm 1 \pmod{8}$, $\equiv b \pmod{P}$
oder $n \equiv \pm 3 \pmod{8}$, $\equiv a \pmod{P}$

und jedem bestimmten Congruenzpaare entspricht eine bestimmte Zahlclasse $n \pmod{8P}$; die Zahlen n vertheilen sich daher in arithmetische Reihen von der Differenz $4D$; jeder der beiden Kategorien gehören gleich viele Zahlclassen an.

Beispiel. Ist $D = -6$, so ergiebt sich

$$\left(\frac{-6}{n}\right) = +1, \quad \text{wenn} \quad n \equiv 1, 5, 7, 11 \pmod{24}$$

$$\left(\frac{-6}{n}\right) = -1, \quad \text{wenn} \quad n \equiv 13, 17, 19, 23 \pmod{24}.$$

IV. $D = \pm 2P \equiv 6 \pmod{8}$

In diesem Falle ist

$$\left(\frac{D}{n}\right) = (-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right),$$

und folglich

$$\left(\frac{D}{n}\right) = +1, \quad \text{wenn} \quad n \equiv 1, 3 \pmod{8}, \equiv a \pmod{P}$$
$$\text{oder} \quad n \equiv 5, 7 \pmod{8}, \equiv b \pmod{P}$$

dagegen

$$\left(\frac{D}{n}\right) = -1, \quad \text{wenn} \quad n \equiv 1, 3 \pmod{8}, \equiv b \pmod{P}$$
$$\text{oder} \quad n \equiv 5, 7 \pmod{8}, \equiv a \pmod{P}.$$

Die Zahlen n vertheilen sich wieder in arithmetische Reihen von der Differenz $4D$; jeder der beiden Kategorien gehören gleich viele Zahlclassen an.

Beispiel. Für $D = +6$ ergiebt sich

$$\left(\frac{6}{n}\right) = +1, \quad \text{wenn} \quad n \equiv 1, 5, 19, 23 \pmod{24}$$

$$\left(\frac{6}{n}\right) = -1, \quad \text{wenn} \quad n \equiv 7, 11, 13, 17 \pmod{24}.$$

Wir bemerken schliesslich, dass die vier Fälle sich zusammenfassen lassen, wenn man zwei positive oder negative Einheiten δ, ε einführt, so, dass $\delta = +1$ oder $= -1$, je nachdem $\pm P \equiv 1$ oder $\equiv 3 \pmod{4}$, und dass $\varepsilon = +1$ oder $= -1$, je nachdem D ungerade oder gerade ist. Die vier Fälle stellen sich dann folgendermassen dar:

$$D = \pm P \equiv 1 \pmod{4}, \quad \delta = +1, \quad \varepsilon = +1;$$
$$D = \pm P \equiv 3 \pmod{4}, \quad \delta = -1, \quad \varepsilon = +1;$$
$$D = \pm 2P \equiv 2 \pmod{8}, \quad \delta = +1, \quad \varepsilon = -1;$$
$$D = \pm 2P \equiv 6 \pmod{8}, \quad \delta = -1, \quad \varepsilon = -1.$$

Dann ist vermöge des allgemeinen Reciprocitätssatzes und der Ergänzungssätze (§. 46)

$$\left(\frac{D}{n}\right) = \delta^{1/2(n-1)}\,\varepsilon^{1/8(n^2-1)}\left(\frac{n}{P}\right),$$

wo n wieder irgend eine positive relative Primzahl zu $2D$ bedeutet.

Lässt man n ein vollständiges System incongruenter Zahlen nach dem Modulus $4D$ durchlaufen, welche zugleich positiv und relative Primzahlen zu $2D$ sind, so ergiebt sich in allen vier Fällen, dass die entsprechende Summe

$$\Sigma\left(\frac{D}{n}\right) = 0$$

ist; im ersten Falle genügt es schon, dass n ein solches vollständiges Restsystem nach dem Modulus $2D$ durchläuft.

Vierter Abschnitt.

Von den quadratischen Formen.

§. 53.

Unter einer *Form* versteht man in der Zahlentheorie im Allgemeinen eine ganze rationale Function von Variabeln, deren Coefficienten ganze Zahlen sind (vergl. §. 39). Je nach dem Grade derselben unterscheidet man *lineare*, *quadratische*, *cubische* Formen u. s. w.; je nach der Anzahl der vorkommenden Variabeln spricht man von *binären*, *ternären* Formen u. s. w. Wir werden uns im Folgenden ausschliesslich mit Ausdrücken von der Form

$$ax^2 + 2bxy + cy^2$$

beschäftigen, wo a, b, c bestimmte, gegebene ganze Zahlen, x und y aber unbestimmte, variabele ganze Zahlen bedeuten; und wir werden diese homogenen binären quadratischen Formen, wo kein Missverständniss zu besorgen ist, kurz Formen nennen.

Wir haben dem Coefficienten des Productes xy der beiden Variabeln gleich die Gestalt einer geraden Zahl $2b$ gegeben, weil die Untersuchung dadurch erleichtert wird; sollte in einer Form dieser Coefficient eine ungerade Zahl sein, so würde es genügen, die ganze Form mit 2 zu multipliciren, um diesen Fall auf den obigen zurückzuführen, und aus den Eigenschaften der so erhaltenen Form würde man mit Leichtigkeit auf die Eigenschaften der ursprünglichen Form zurückschliessen können.

Sind die drei Glieder in der obigen Anordnung geschrieben, so nennt man a den *ersten*, b (nicht $2b$) den *zweiten*, c den *dritten Coefficienten*; a und c fasst man auch wohl unter dem gemeinschaftlichen Namen der *äusseren* Coefficienten zusammen, und nennt dann b im Gegensatz den *mittlern* Coefficienten; ähnlich heisst x die *erste*, y die *zweite Variabele*. Eine solche Form bezeichnet man wohl auch kurz durch das Symbol (a, b, c), wenn es sich nur darum handelt, die Coefficienten anzugeben, von denen allein die Eigenschaften der Form abhängen können.

Wir schliessen nun ein für alle Mal die Fälle aus, in welchen die Form sich in zwei lineare Factoren mit *rationalen* Coefficienten zerfällen lässt, weil diese eine andere und zwar einfachere Behandlung gestatten. Zunächst folgt hieraus, dass in den Formen, mit welchen allein wir uns beschäftigen wollen, keiner der äusseren Coefficienten gleich Null sein wird; da ferner

$$ax^2 + 2bxy + cy^2 = \frac{1}{a}\left((ax + by)^2 - (b^2 - ac)y^2\right)$$

ist, so ergiebt sich weiter, dass die Zahl $b^2 - ac$ nie eine vollständige Quadratzahl sein darf, denn sonst würde die Form

$$ax^2 + 2bxy + cy^2 =$$

$$\frac{1}{a}\left(ax + (b + \sqrt{b^2 - ac})\, y\right)\left(ax + (b - \sqrt{b^2 - ac})\, y\right)$$

ein Product aus zwei linearen Factoren mit rationalen Coefficienten sein. Die Zahl $b^2 - ac$, von welcher, wie wir sehen werden, die Eigenschaften der Form (a, b, c) hauptsächlich abhängen, heisst die *Determinante* *) dieser Form; wir werden sie im Folgenden mit dem Buchstaben D bezeichnen. Die unseren Formen (a, b, c) auferlegte Beschränkung besteht also darin, dass *D kein Quadrat* ist.

Euler hat sich zuerst mit solchen Formen, aber nur von specieller Natur, beschäftigt; erst *Lagrange* legte den Grund zu einer allgemeinen Theorie derselben, die dann später von *Legendre*, vor Allen aber durch *Gauss* vervollständigt wurde.

Ihre Entstehung verdankt die ganze Theorie dem Probleme, zu entscheiden, ob eine gegebene Zahl m durch die gegebene Form (a,b,c) *darstellbar* ist, d. h. ob es specielle Werthe von x, y giebt, für welche die Form den Werth m erhält. Doch ist zur vollständigen

---

*) *Gauss: D. A.* art. 154.

Lösung desselben die Theorie der *Transformation* erforderlich, mit welcher wir uns zunächst beschäftigen wollen.

§. 54.

Ebenso wie die Gleichungen der Curven in der analytischen Geometrie ihre Gestalt ändern, wenn ein anderes Coordinatensystem gewählt wird, so geht eine quadratische Form (a, b, c) durch Einführung zweier neuen Variabeln in eine neue quadratische Form (a', b', c') über. Sind nämlich x, y die Variabeln der Form (a, b, c), und setzt man

$$\begin{aligned} x &= \alpha x' + \beta y', \\ y &= \gamma x' + \delta y', \end{aligned} \qquad (1)$$

wo $\alpha, \beta, \gamma, \delta$ vier bestimmte ganze Zahlen, und x', y' die neuen Variabeln bedeuten, so wird

$$ax^2 + 2bxy + cy^2 = a'x'^2 + 2b'x'y' + c'y'^2,$$

und die Coefficienten a', b', c' der neuen quadratischen Form hängen auf folgende Weise von denen der ursprünglichen Form und von den vier Coefficienten $\alpha, \beta, \gamma, \delta$ ab:

$$\begin{aligned} a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2. \end{aligned} \qquad (2)$$

Man drückt den Zusammenhang der beiden Formen kurz so aus: die Form $ax^2 + 2bxy + cy^2$ geht durch die *Transformation* oder *Substitution* (1) in die Form $a'x'^2 + 2b'x'y' + c'y'^2$ über. Die Zahlen $\alpha, \beta, \gamma, \delta$ heissen der Reihe nach der *erste*, *zweite*, *dritte*, *vierte Coefficient* der Substitution. Da die Wahl der Buchstaben zur Bezeichnung der Variabeln von ganz untergeordneter Bedeutung ist, und die Natur der Formen und Substitutionen nur von den Coefficienten abhängt, so drückt man sich häufig noch kürzer so aus: die Form (a, b, c) geht durch die Substitution $\alpha, \beta, \gamma, \delta$ oder $\binom{\alpha, \beta}{\gamma, \delta}$ in die Form (a', b', c') über; und diese Ausdrucksweise soll nicht mehr oder weniger sagen, als dass die drei Gleichungen (2) Statt finden. Hierbei ist wohl auf die Stellung der Coefficienten der Formen sowohl, wie derjenigen der Substi-

tution zu achten; behalten wir die eben eingeführten Bezeichnungen bei, so müssen wir z. B. sagen, dass gleichzeitig die Form

(a, b, c) durch die Substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ in (a', b', c'),

(a, b, c) „ „ „ $\begin{pmatrix}\beta, & \alpha \\ \delta, & \gamma\end{pmatrix}$ „ (c', b', a'),

(c, b, a) „ „ „ $\begin{pmatrix}\gamma, & \delta \\ \alpha, & \beta\end{pmatrix}$ „ (a', b', c'),

(c, b, a) „ „ „ $\begin{pmatrix}\delta, & \gamma \\ \beta, & \alpha\end{pmatrix}$ „ (c', b', a')

übergeht.

Es leuchtet ein, dass jede durch die zweite Form (a', b', c') darstellbare Zahl auch durch die erste Form (a, b, c) dargestellt werden kann; denn wird die Zahl m durch (a', b', c') dargestellt, indem den Variabeln x', y' die speciellen Werthe r', s' ertheilt werden, so setze man

$$r = \alpha r' + \beta s', \quad s = \gamma r' + \delta s',$$

und es wird die Form (a, b, c) dieselbe Zahl m darstellen, sobald $x = r$, $y = s$ gesetzt wird. Man sagt deshalb auch: die Form (a, b, c) *enthält* die Form (a', b', c'), oder deutlicher: die Form (a', b', c') ist unter der Form (a, b, c) *enthalten**); eben weil sämmtliche durch (a', b', c') darstellbare Zahlen unter den durch (a, b, c) darstellbaren enthalten sind**).

Von besonderer Wichtigkeit ist die Relation, in welcher die Determinante

$$D' = b'^2 - a'c'$$

der neuen Form zu der der früheren steht; substituirt man für a', b', c' ihre Ausdrücke gemäss den Gleichungen (2), so findet man nach leichten Reductionen

$$D' = (\alpha\delta - \beta\gamma)^2 D;$$

die neue Determinante ist daher stets gleich der alten, multiplicirt mit einer Quadratzahl; beide Determinanten haben also auch dasselbe Vorzeichen. Da wir von vorn herein Formen ausschliessen, deren

*) *Gauss: D. A.* art. 157.

**) Ueber die Umkehrung dieses Satzes siehe *Schering: Théorèmes relatifs aux formes binaires quadratiques qui représentent les mêmes nombres,* Journal de Mathématiques publ. p. Liouville T. IV. 2e série. 1859.

Determinanten $= 0$ sind, so betrachten wir deshalb auch nur solche Substitutionen $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$, für welche die Coefficientenverbindung $\alpha\delta - \beta\gamma$ (die sogenannte *Determinante der Substitution*) einen von Null verschiedenen Werth hat. Hieran knüpft sich jedoch noch eine wichtige Unterscheidung; je nachdem nämlich dieser Ausdruck $\alpha\delta - \beta\gamma$ einen positiven oder negativen Werth hat, soll die Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$ eine *eigentliche* oder *uneigentliche* heissen, und diese Ausdrucksweise soll auf die Beziehung zwischen den Formen (a, b, c) und (a', b', c') übertragen werden, indem wir sagen, dass die Form (a', b', c') *eigentlich* oder *uneigentlich* unter der Form (a, b, c) *enthalten* sei, je nachdem die Substitution $\left(\begin{smallmatrix}\alpha, & \beta\\ \gamma, & \delta\end{smallmatrix}\right)$, durch welche die letztere in die erstere übergeht, eigentlich oder uneigentlich ist. Um Missverständnisse zu vermeiden, fügen wir sogleich hinzu, dass eine Form eine andere sowohl eigentlich als auch uneigentlich enthalten kann; denn es tritt häufig der Fall ein, dass eine Form einmal durch eine eigentliche, ein anderes Mal durch eine uneigentliche Substitution in eine und dieselbe zweite Form transformirt wird. So z. B. geht die Form $(3, 13, 18)$ durch die eigentliche Substitution $\left(\begin{smallmatrix}+1, & 0\\ -1, & +1\end{smallmatrix}\right)$, und ebenso durch die uneigentliche Substitution $\left(\begin{smallmatrix}+1, & +2\\ -1, & -3\end{smallmatrix}\right)$ in die andere Form $(-5, -5, 18)$ über; die erstere enthält daher die letztere sowohl eigentlich als auch uneigentlich.

Man nennt ferner zwei Substitutionen *gleichartig*, wenn sie beide eigentlich, oder beide uneigentlich sind, *ungleichartig*, wenn die eine eigentlich, die andere uneigentlich ist.

§. 55.

Behalten wir die vorhergehenden Bezeichnungen bei, und nehmen wir an, dass die Form

$$(a', b', c') = a'x'^2 + 2b'x'y' + c'y'^2$$

durch eine neue Substitution

$$x' = \alpha'x'' + \beta'y''$$
$$y' = \gamma'x'' + \delta'y''$$

in die Form

$$(a'', b'', c'') = a''x''^2 + 2b''x''y'' + c''y''^2$$

übergeht, so geht offenbar die erste Form (a, b, c) durch die Substitution

$$x = \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y'')$$
$$y = \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'')$$

oder

$$x = (\alpha\alpha' + \beta\gamma') x'' + (\alpha\beta' + \beta\delta') y''$$
$$y = (\gamma\alpha' + \delta\gamma') x'' + (\gamma\beta' + \delta\delta') y''$$

in die dritte Form (a'', b'', c'') über. Hieraus folgt der Satz:

Enthält eine Form eine zweite, diese wieder eine dritte, so enthält auch die erste Form die dritte.

Bezeichnet man nun die Coefficientenverbindung

$$(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma')$$

mit ε, so ist nothwendig die Determinante der dritten Form $D'' = \varepsilon^2 D$; da aber andererseits

$$D' = (\alpha\delta - \beta\gamma)^2 D, \; D'' = (\alpha'\delta' - \beta'\gamma')^2 D',$$

also auch

$$D'' = (\alpha\delta - \beta\gamma)^2 (\alpha'\delta' - \beta'\gamma')^2 D,$$

und D von Null verschieden ist, so schliessen wir hieraus, dass

$$\varepsilon^2 = (\alpha\delta - \beta\gamma)^2 (\alpha'\delta' - \beta'\gamma')^2$$

ist, und man überzeugt sich leicht durch Vergleichung beider Seiten, dass die Quadratwurzel in folgender Weise auszuziehen ist:

$$\varepsilon = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma').$$

Aus dieser Gleichung (welche einen der einfachsten Sätze der Determinantentheorie enthält) folgt noch eine wesentliche Vervollständigung des obigen Satzes, nämlich:

Die erste Form enthält die dritte eigentlich oder uneigentlich, je nachdem die erste die zweite in derselben oder in entgegengesetzter Art enthält, wie die zweite die dritte.

Fährt man in derselben Weise fort und transformirt die dritte Form in eine vierte, diese in eine fünfte u. s. f., so ergiebt sich unmittelbar der allgemeine Satz: *Wenn von einer Reihe von Formen jede die nächstfolgende enthält, so enthält die erste Form auch die letzte, und zwar eigentlich oder uneigentlich, je nachdem die Anzahl der hierbei auftretenden uneigentlichen Substitutionen gerade oder ungerade ist.*

Die Substitution, durch welche die erste Form unmittelbar in die letzte transformirt wird, heisst *zusammengesetzt* aus den einzelnen successiven Substitutionen; um die Zusammensetzung von

zwei Substitutionen anzudeuten, wollen wir uns bisweilen der Bezeichnung

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix} = \begin{pmatrix}\alpha\alpha' + \beta\gamma', & \alpha\beta' + \beta\delta'\\ \gamma\alpha' + \delta\gamma', & \gamma\beta' + \delta\delta'\end{pmatrix}$$

bedienen; offenbar ist es im Allgemeinen nicht erlaubt, die Ordnung der beiden successiven Substitutionen umzukehren, weil hierdurch auch die resultirende Substitution geändert würde. So ist z. B. $\left(\begin{smallmatrix}+1, & 0\\ -1, & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}+1, & +2\\ -1, & -3\end{smallmatrix}\right) = \left(\begin{smallmatrix}+1, & +2\\ -2, & -5\end{smallmatrix}\right)$, dagegen $\left(\begin{smallmatrix}+1, & +2\\ -1, & -3\end{smallmatrix}\right)\left(\begin{smallmatrix}+1, & 0\\ -1, & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}-1, & +2\\ +2, & -3\end{smallmatrix}\right)$.

Dagegen ist es bei drei successiven Substitutionen S, S', S'' gleichgültig, ob man erst S und S' zusammensetzt, und dann das Resultat SS' mit S'' verbindet, oder ob man S mit dem Resultat $S'S''$ der zweiten und dritten Substitution zusammensetzt; in Zeichen:

$$(SS')S'' = S(S'S'').$$

Dies folgt unmittelbar aus dem Begriffe dieser Zusammensetzung; denn sind (x, y), (x', y'), (x'', y'') und (x''', y''') die successiven Variabeln, so ist es für die Ausdrücke von x, y durch x''', y''' gleichgültig, ob man die Variabeln x'', y'' oder die Variabeln x', y' als Zwischenglieder einschiebt.

Ferner ist für die Folge zu bemerken, dass die Substitution $\left(\begin{smallmatrix}1, & 0\\ 0, & 1\end{smallmatrix}\right)$ bei der Zusammensetzung stets fortgelassen werden darf, da sie keine Aenderung hervorbringt.

Endlich leuchtet ein, dass der obige Satz auch so ausgesprochen werden kann: *Die aus den Substitutionen S, S', S'' . . . zusammengesetzte Substitution $SS'S''$ . . . ist eigentlich oder uneigentlich, je nachdem die Anzahl der unter ihnen befindlichen uneigentlichen Substitutionen gerade oder ungerade ist.*

§. 56.

Besonders wichtig ist nun die Frage: wann enthalten zwei Formen sich gegenseitig? Offenbar ist dann das System aller durch die eine Form darstellbaren Zahlen identisch mit dem System derjenigen Zahlen, welche durch die andere Form dargestellt werden können. Zwei solche Formen werden wir *äquivalent* *) nennen. Sind D, D' ihre Determinanten, so muss sowohl $D':D$, als auch

*) *Gauss*: *D. A.* art. 157.

$D:D'$, eine ganze Quadratzahl, also eine ganze positive Zahl sein, und hieraus folgt als eine für die Aequivalenz zweier Formen *erforderliche* Bedingung, dass ihre Determinanten D und D' gleich sein müssen.

Diese Bedingung ist aber umgekehrt *nicht hinreichend*, um auf die Aequivalenz schliessen zu können. Dies ist erst dann gestattet, wenn man ausserdem weiss, dass die eine der beiden Formen die andere enthält. In der That, wenn die beiden Formen (a, b, c) und (a', b', c') gleiche Determinanten haben, und wenn ausserdem die erstere durch die Substitution

$$x = \alpha x' + \beta y'$$
$$y = \gamma x' + \delta y'$$

in die letztere übergeht, so folgt aus der Relation

$$D' = (\alpha\delta - \beta\gamma)^2 D$$

und der Gleichheit von D' und D die Gleichung

$$\alpha\delta - \beta\gamma = \pm 1$$

und hieraus, wenn man zur Abkürzung $\alpha\delta - \beta\gamma = \pm 1 = \varepsilon$ setzt,

$$x' = + \varepsilon\delta x - \varepsilon\beta y$$
$$y' = - \varepsilon\gamma x + \varepsilon\alpha y$$

und es geht daher durch diese Substitution mit ganzzahligen Coefficienten die Form (a', b', c') in die Form (a, b, c) über; also sind in der That beide Formen einander äquivalent. Die Substitutionen

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \text{ und } \begin{pmatrix} + \varepsilon\delta, & - \varepsilon\beta \\ - \varepsilon\gamma, & + \varepsilon\alpha \end{pmatrix},$$

deren jede die *inverse* der andern heisst, und durch deren Zusammensetzung immer die Substitution $\binom{1,\ 0}{0,\ 1}$ entsteht, sind offenbar entweder beide eigentlich, oder beide uneigentlich; je nachdem das Eine oder das Andere Statt findet, sollen die beiden Formen *eigentlich* oder *uneigentlich äquivalent**) heissen.

Sowie wir eben gesehen haben, dass die eine von zwei äquivalenten Formen in die andere immer durch eine Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ übergeht, in welcher $\alpha\delta - \beta\gamma = \pm 1$ ist, so leuchtet auch umgekehrt ein, dass durch jede solche Substitution eine beliebige Form nothwendig in eine ihr äquivalente transformirt wird; denn die Determinanten beider Formen sind einander gleich. Hierin

*) *Gauss: D. A* art. 158.

besteht also die *erforderliche und hinreichende* Bedingung für die Aequivalenz zweier Formen.

Aus dem Begriffe der Aequivalenz ergiebt sich unmittelbar, dass jede Form sich selbst eigentlich äquivalent ist; denn sie geht durch die eigentliche Substitution $\binom{1,\ 0}{0,\ 1}$ in sich selbst über. Dies ist nur ein specieller Fall des folgenden Satzes, welcher sehr oft zur Anwendung kommen wird: *Wenn zwei Formen* (a, b, c) *und* (a', b', c') *von gleicher Determinante* D *denselben ersten Coefficienten* a *haben, und wenn ihre mittleren Coefficienten* b, b' *einander congruent sind in Bezug auf den Modul* a, *so dass* $b' = a\beta + b$; *so sind die beiden Formen eigentlich äquivalent, und die erstere geht durch die eigentliche Substitution* $\binom{1,\ \beta}{0,\ 1}$ *in die letztere über.*

Ferner bemerke man folgende Fälle der uneigentlichen Aequivalenz: Zwei *entgegengesetzte**) Formen (*formae oppositae*), d. h. zwei Formen (a, b, c) und $(a, -b, c)$, welche sich nur durch das Vorzeichen des mittlern Coefficienten unterscheiden, sind stets *uneigentlich* äquivalent, indem die eine durch die Substitution $\binom{1,\ \ 0}{0,\ -1}$ in die andere übergeht. Dasselbe gilt von zwei *Gefährten***) (*formae sociae*), d. h. von zwei Formen (a, b, c) und (c, b, a), welche dieselben Coefficienten, nur in umgekehrter Folge, haben; die eine geht in die andere durch die Substitution $\binom{0,\ 1}{1,\ 0}$ über.

Aus diesen beiden Fällen folgt wieder durch Zusammensetzung, dass die beiden Formen (a, b, c) und $(c, -b, a)$ *eigentlich* äquivalent sind; denn die erstere geht in die letztere durch die Substitution $\binom{0,\ 1}{-1,\ 0}$ über.

§. 57.

Auch hier bei der Aequivalenz schliesst die eine Art derselben die andere nicht aus; es kommt häufig der Fall vor, dass zwei Formen einander sowohl eigentlich als uneigentlich äquivalent sind; in dem oben (§. 54) angeführten Beispiel sind wirklich die beiden Formen (3, 13, 18) und (— 5, — 5, 18) eigentlich und uneigentlich äquivalent; die erstere geht durch die Substitutionen

*) *Gauss: D. A.* art. 159.

**) *Gauss: D. A.* art. 187.

$\binom{+1,\ 0}{-1,\ 1}$ und $\binom{+1,\ +2}{-1,\ -3}$ in die letztere über, und umgekehrt diese in jene durch die inversen Substitutionen $\binom{1,\ 0}{1,\ 1}$ und $\binom{+3,\ +2}{-1,\ -1}$.

Wenn zwei Formen sowohl eigentlich als uneigentlich äquivalent sind, so ist jede von ihnen sich selbst uneigentlich äquivalent.

Denn, wenn die Form (a, b, c) durch jede der beiden Substitutionen

$$\begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix} \text{ und } \begin{pmatrix}\alpha'', \beta'' \\ \gamma'', \delta''\end{pmatrix},$$

in denen

$$\alpha'\delta' - \beta'\gamma' = +1, \quad \alpha''\delta'' - \beta''\gamma'' = -1,$$

in die Form (a', b', c') übergeht, so geht (a', b', c') durch jede der beiden inversen Substitutionen

$$\begin{pmatrix}+\delta', -\beta' \\ -\gamma', +\alpha'\end{pmatrix} \text{ und } \begin{pmatrix}-\delta'', +\beta'' \\ +\gamma'', -\alpha''\end{pmatrix}$$

in (a, b, c) über; und hieraus folgt, dass (a, b, c) durch jede der beiden zusammengesetzten, und zwar nothwendig uneigentlichen Substitutionen

$$\begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix}\begin{pmatrix}-\delta'', +\beta'' \\ +\gamma'', -\alpha''\end{pmatrix} \text{ und } \begin{pmatrix}\alpha'', \beta'' \\ \gamma'', \delta''\end{pmatrix}\begin{pmatrix}+\delta', -\beta' \\ -\gamma', +\alpha'\end{pmatrix}$$

in sich selbst übergeht. So z. B. geht die Form (3, 13, 18) durch die uneigentlichen Substitutionen $\binom{+1,\ 0}{-1,\ 1}\binom{+3,\ +2}{-1,\ -1} = \binom{+3,\ +2}{-4,\ -3}$ und $\binom{+1,\ +2}{-1,\ -3}\binom{1,\ 0}{1,\ 1} = \binom{+3,\ +2}{-4,\ -3}$ in sich selbst über.

Es ist kein Zufall, dass diese beiden auf verschiedene Art zusammengesetzten Substitutionen identisch ausfallen; setzt man nämlich

$$\begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix}\begin{pmatrix}-\delta'', +\beta'' \\ +\gamma'', -\alpha''\end{pmatrix} = \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix},$$

so findet man zunächst

$$\begin{pmatrix}\alpha'', \beta'' \\ \gamma'', \delta''\end{pmatrix}\begin{pmatrix}+\delta', -\beta' \\ -\gamma', +\alpha'\end{pmatrix} = \begin{pmatrix}-\delta, +\beta \\ +\gamma, -\alpha\end{pmatrix},$$

und wir haben daher, um die Identität dieser beiden Substitutionen nachzuweisen, nur noch zu zeigen, dass in jeder uneigentlichen Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$, durch welche eine Form in sich selbst übergeht, stets der erste und vierte Coefficient einander gleich, aber entgegengesetzt sind. Dies geschieht leicht auf folgende Weise. Wenn die Form (a, b, c) durch die uneigentliche Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ in sich selbst übergeht, so ist

$$a\alpha^2 + (2b\alpha + c\gamma)\gamma = a$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b$$
$$\alpha\delta - \beta\gamma = -1.$$

Die zweite dieser drei Gleichungen geht, wenn man der dritten gemäss $\beta\gamma$ durch $\alpha\delta + 1$ ersetzt, in folgende über:

$$a\alpha\beta + (2b\alpha + c\gamma)\delta = 0;$$

eliminirt man aus dieser und aus der ersten jener drei Gleichungen die Grösse $2b\alpha + c\gamma$, so erhält man, wenn man den Factor a wegwirft (der ja von Null verschieden ist, weil sonst die Determinante D eine Quadratzahl wäre), die Relation

$$(\alpha^2 - 1)\delta = \alpha\beta\gamma,$$

woraus mit Rücksicht auf $\alpha\delta - \beta\gamma = -1$ wirklich folgt, dass $\delta = -\alpha$ ist, was zu beweisen war.

§. 58.

Jede uneigentliche Substitution, durch welche eine Form (a, b, c) in sich selbst übergeht, ist daher nothwendig von der Form $\binom{\alpha,\ +\beta}{\gamma,\ -\alpha}$, und es ist also gleichzeitig $\alpha^2 + \beta\gamma = 1$. Von besonderm Interesse ist der specielle Fall $\gamma = 0$; dann ist $\alpha = \pm 1$ und entsprechend $\pm\, a\beta = 2b$; eine solche Form, deren doppelter mittlerer Coefficient durch den ersten theilbar ist, soll eine *ambige* Form (*forma anceps*) heissen*). Und umgekehrt ist leicht zu sehen, dass jede ambige Form sich selbst uneigentlich äquivalent ist; denn wenn (a, b, c) eine solche Form, und also $2b = a\beta$ ist, so geht (a, b, c) wirklich durch die uneigentliche Substitution $\binom{1,\ +\beta}{0,\ -1}$ in sich selbst über. Dasselbe gilt offenbar von jeder Form, welche einer ambigen Form äquivalent ist; aber es besteht auch der umgekehrte Satz:**)

Wenn eine Form sich selbst uneigentlich äquivalent ist, so giebt es stets eine ihr äquivalente ambige Form.

Beweis. Es sei φ eine solche Form, welche durch die uneigentliche Substitution $\binom{\alpha,\ +\beta}{\gamma,\ -\alpha}$ in sich selbst übergeht; ist $\gamma = 0$, so wissen wir, dass φ selbst eine ambige Form, und folglich der Satz richtig ist. Ist aber γ von Null verschieden, so suchen wir eine eigentliche Substitution $\binom{\lambda,\ \mu}{\nu,\ \varrho}$, durch welche die Form φ in eine ihr äquivalente ambige Form übergeht, die wir mit ψ bezeichnen wollen. Da also $\lambda\varrho - \mu\nu = +1$, und folglich ψ durch die

*) *Gauss: D. A.* art. 163. Vergl. *Kummer* im Monatsbericht der Berliner Akademie vom 18. Februar 1858.

**) *Gauss: D. A.* art. 164.

inverse Substitution $\begin{pmatrix} +\varrho, & -\mu \\ -\nu, & +\lambda \end{pmatrix}$ in φ übergeht, so muss ψ durch die offenbar uneigentliche, aus den drei successiven Substitutionen

$$\begin{pmatrix} +\varrho, & -\mu \\ -\nu, & +\lambda \end{pmatrix}, \; \begin{pmatrix} \alpha, & +\beta \\ \gamma, & -\alpha \end{pmatrix}, \; \begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix}$$

zusammengesetzte Substitution in sich selbst übergehen. Der dritte Coefficient dieser Substitution ist

$$\gamma\lambda^2 - 2\alpha\lambda\nu - \beta\nu^2,$$

und es kommt nur darauf an, zwei relative Primzahlen λ, ν so zu bestimmen, dass dieser Coefficient $= 0$ wird; denn dann ist ψ eine ambige Form. Diese Forderung reducirt sich, wenn man mit γ multiplicirt und bedenkt, dass $\alpha^2 + \beta\gamma = 1$ ist, auf die folgende:

$$(\gamma\lambda - \alpha\nu)^2 - \nu^2 = 0; \; \frac{\lambda}{\nu} = \frac{\alpha \pm 1}{\gamma} = \frac{-\beta}{\alpha \mp 1};$$

da unserer Annahme nach γ von Null verschieden ist, so kann man also λ und ν dieser Forderung gemäss bestimmen, und zwar als relative Primzahlen, wenn man den Bruch $(\alpha \pm 1) : \gamma$ auf seine kleinste Benennung $\lambda : \nu$ bringt. Dies Letztere ist erforderlich, weil ja die vier Coefficienten λ, μ, ν, ϱ der Gleichung $\lambda\varrho - \mu\nu = 1$ genügen müssen. Sobald nun λ und ν auf dem angegebenen Wege bestimmt sind, so kann man dann unendlich viele Werthenpaare für ϱ und μ (nach §. 24) finden, welche diese letzte Forderung erfüllen. Auf diese Weise ist also wirklich aus $\begin{pmatrix} \alpha, & +\beta \\ \gamma, & -\alpha \end{pmatrix}$ eine eigentliche Substitution $\begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix}$ gefunden, welche die gegebene Form φ in eine ihr äquivalente ambige Form ψ transformirt, und hierdurch der obige Satz bewiesen.

Nehmen wir als Beispiel die obige Form (3, 13, 18), welche durch die uneigentliche Substitution $\begin{pmatrix} +3, & +2 \\ -4, & -3 \end{pmatrix}$ in sich selbst übergeht; wir haben also nur

$$\frac{\lambda}{\nu} = \frac{3 \pm 1}{-4}$$

zu setzen; nehmen wir das obere Zeichen, so ist $\lambda = \pm 1$, $\nu = \mp 1$ zu setzen, und entsprechend $\varrho + \mu = \pm 1$. Nehmen wir die obern Zeichen und $\varrho = 1$, $\mu = 0$, so erhalten wir die Substitution $\begin{pmatrix} +1, & 0 \\ -1, & 1 \end{pmatrix}$, durch welche, wie schon oben bemerkt ist, die Form (3, 13, 18) in die Form (—5, —5, 18) übergeht, welche in der That eine ambige Form ist.

Ferner: Die Form (7, 1, —1) geht durch die uneigentliche

Substitution $\binom{+2,\ +1}{-3,\ -2}$ in sich selbst über; in diesem Fall haben wir also

$$\frac{\lambda}{\nu} = \frac{2 \pm 1}{-3}$$

zu setzen; nehmen wir der Einfachheit halber wieder das obere Zeichen, so können wir wieder $\lambda = 1$, $\nu = -1$, $\varrho = 1$, $\mu = 0$ setzen; und in der That geht die Form $(7, 1, -1)$ durch die Substitution $\binom{+1,\ 0}{-1,\ 1}$ in die ambige Form $(4, 2, -1)$ über.

§. 59.

Wir verlassen hiermit diesen interessanten Gegenstand und beschäftigen uns von jetzt an ausschliesslich mit der *eigentlichen* Aequivalenz; nur diese soll im Folgenden gemeint sein, wenn schlechthin von Aequivalenz gesprochen wird; ebenso soll unter Substitution immer nur noch die *eigentliche* Substitution verstanden sein. Werden daher zwei Formen f, f' äquivalent genannt, so bedeutet dieser Ausdruck stets (§. 56), dass eine Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ existirt, deren Coefficienten der Bedingung $\alpha\delta - \beta\gamma = +1$ genügen, und durch welche f in f' übergeht; umgekehrt geht dann f' in f über durch die inverse Substitution $\binom{\delta,\ -\beta}{-\gamma,\ \alpha}$, deren Coefficienten derselben Bedingung $\delta\alpha - (-\beta)(-\gamma) = +1$ genügen. Aus dem allgemeinen Satze des §. 55 geht nun folgender specielle hervor: *Sind zwei Formen einer dritten äquivalent, so sind sie auch einander äquivalent*; und dieser Satz bildet die Grundlage für den wichtigsten Begriff in der ganzen Theorie der quadratischen Formen.

Es sei f eine bestimmte gegebene Form von der Determinante D, und F der Inbegriff aller der Formen $f, f', f'' \ldots$, welche mit f äquivalent sind; zufolge des eben erwähnten Satzes sind nun je zwei in dem System F vorkommende Formen f', f'' ebenfalls äquivalent; ist daher f' irgend eine in F vorkommende Form, so ist das System aller mit f' äquivalenten Formen identisch mit dem System F. Ein solches System unter einander äquivalenter Formen soll eine *Classe von Formen* *) oder eine *Formenclasse* heissen, und es leuchtet ein, dass durch irgend ein Individuum einer solchen Classe alle anderen derselben Classe angehörenden Formen vollständig be-

*) *Gauss: D. A.* art. 223.

stimmt sind; man kann daher immer ein solches Individuum als *Repräsentanten der Formenclasse* ansehen.

Es würde nicht schwer sein zu beweisen, dass es in jeder solchen Formenclasse unendlich viele Individuen giebt, d. h. dass die Anzahl der Formen, in welche eine gegebene Form f durch die unendlich vielen verschiedenen Substitutionen $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ übergeht, in denen $\alpha\delta - \beta\gamma = +1$, unendlich gross ist, obgleich es vorkommen kann, und zwar bei positiven Determinanten immer vorkommt, dass unendlich viele von diesen Substitutionen die Form f nur in eine und dieselbe Form f' transformiren; allein dieser Nachweis hat für uns zunächst kein Interesse. Von grösserer Wichtigkeit und von dem grössten Interesse ist dagegen die folgende Betrachtung.

Denkt man sich alle Formen von einer und derselben Determinante D in ihre verschiedenen Classen eingetheilt, und wählt man aus jeder Classe nach Belieben eine Form als Repräsentanten derselben, so erhält man ein sogenanntes *vollständiges System nicht äquivalenter Formen* für diese Determinante D; die fundamentale und vollständig charakteristische Eigenschaft eines solchen vollständigen Formensystems S besteht darin, dass jede beliebige Form von der Determinante D stets einer, aber auch nur einer von den in diesem System S enthaltenen Formen äquivalent ist. Die Anzahl dieser verschiedenen Classen (und also auch ihrer Repräsentanten in dem vollständigen Formensystem S) ist nun, wie sich zunächst für negative, später auch für positive Determinanten herausstellen wird, eine *endliche*, und wir bezeichnen absichtlich schon jetzt die genaue Bestimmung dieser *Classenanzahl für eine gegebene Determinante*, welche innig mit den schönsten algebraischen und analytischen Untersuchungen dieses Jahrhunderts verknüpft ist, als die letzte und hauptsächlichste von uns zu lösende Aufgabe.

Der Weg zu diesem Ziele wird gebahnt durch die Lösung der beiden folgenden Hauptprobleme in der Theorie der Aequivalenz:

I. *Zu entscheiden, ob zwei gegebene Formen von gleicher Determinante äquivalent sind, also derselben Classe angehören, oder nicht.*

II. *Alle Substitutionen zu finden, durch welche die eine von zwei gegebenen äquivalenten Formen in die andere übergeht.*

Es wird aber gut sein, die Beschäftigung mit diesen beiden Problemen dadurch zu motiviren, dass wir zeigen, wie die Theorie der *Darstellung* der Zahlen durch quadratische Formen vollständig

auf dieselben zurückgeführt werden kann; und so schicken wir im Folgenden einige Hauptsätze dieser Theorie voraus.

§. 60.

Man nennt, wie schon im Anfang dieses Abschnittes erwähnt ist, eine ganze Zahl m *darstellbar* durch die quadratische Form (a, b, c), wenn es zwei ganze Zahlen x, y giebt, welche der Gleichung

$$ax^2 + 2bxy + cy^2 = m \tag{1}$$

genügen. Wir können uns aber zunächst auf sogenannte *eigentliche Darstellungen* (x, y) beschränken, in welchen die beiden *darstellenden Zahlen* x, y *relative Primzahlen* sind; denn ist δ der grösste gemeinschaftliche Divisor von x und y, so ist m nothwendig theilbar durch δ^2; setzt man nun $x = x'\delta$, $y = y'\delta$ und $m = m'\delta^2$, so wird m' offenbar durch die Form (a, b, c) dargestellt, wenn x' und y' als darstellende Zahlen genommen werden. Da nun die letztern relative Primzahlen sind, so erkennt man leicht, dass, sobald alle eigentlichen Darstellungen der Zahlen bekannt sind, hieraus die übrigen (*uneigentlichen*) Darstellungen leicht gefunden werden können; wir schliessen daher die letztern von unserer jetzigen Betrachtung ganz aus. Dies vorausgeschickt, schreiten wir zur Erforschung der erforderlichen und hinreichenden Bedingungen für die Darstellbarkeit einer gegebenen Zahl m durch eine gegebene Form (a, b, c).

1. Wir nehmen also an, die obige Darstellung (1) der Zahl m durch die Form (a, b, c) von der Determinante $D = b^2 - ac$ sei eine eigentliche, d. h. x und y seien relative Primzahlen. Dann giebt es (nach §§. 22, 24) immer unendlich viele Paare von ganzen Zahlen ξ, η, welche der unbestimmten Gleichung ersten Grades

$$x\eta - y\xi = +1 \tag{2}$$

Genüge leisten. Wählen wir ein solches Paar ξ, η nach Belieben aus, so geht (nach §. 56) die Form (a, b, c) durch die Substitution $\binom{x,\ \xi}{y,\ \eta}$ in eine äquivalente Form (m, n, l) über, deren erster Coefficient zufolge (1) die dargestellte Zahl m ist; der mittlere Coefficient wird

$$n = (ax + by)\xi + (bx + cy)\eta, \tag{3}$$

und der dritte Coefficient l ergiebt sich, da beide Formen (nach §. 56) dieselbe Determinante haben, aus der Gleichung $n^2 - ml = D$ (denn m kann nicht $= 0$ sein, weil sonst D ein Quadrat wäre). Da nun dieser dritte Coefficient l nothwendig eine ganze Zahl ist, so folgt, *dass D quadratischer Rest von m, und dass $z = n$ eine Wurzel der Congruenz*

$$z^2 \equiv D \,(\text{mod. } m) \tag{4}$$

ist.

2. Gesetzt nun, man nimmt statt der beiden Zahlen ξ, η irgend ein anderes Paar von Zahlen ξ', η', welche derselben Bedingung (2) genügen, so geht die Form (a, b, c) durch die Substitution $\binom{x,\ \xi'}{y,\ \eta'}$ ebenfalls in eine äquivalente Form (m, n', l') über, und man erhält wieder eine Wurzel

$$n' = (ax + by)\,\xi' + (bx + cy)\,\eta'$$

der Congruenz (4). Es ist nun von Wichtigkeit zu untersuchen, in welcher Beziehung diese zu der früheren steht. Da der Voraussetzung nach $x\eta - y\xi = 1 = x\eta' - y\xi'$, also auch $x(\eta' - \eta) = y(\xi' - \xi)$ ist, und x und y relative Primzahlen sind, so muss $\xi' - \xi$ durch x theilbar sein; nennen wir den Quotienten v, so folgt

$$\xi' = \xi + xv, \quad \eta' = \eta + yv;$$

alle denkbaren Auflösungen der Gleichung (2) sind daher in diesen Formeln enthalten, in welchen v jede beliebige ganze Zahl bedeutet; und umgekehrt, jedem ganzzahligen Werthe von v entsprechen zwei Zahlen ξ', η', welche der Gleichung (2) genügen. (Dies gilt selbst dann noch, wenn eine der beiden Zahlen x, y gleich Null, und folglich die andere $= \pm 1$ ist.) Substituirt man nun die vorstehenden Ausdrücke in den von n', so erhält man, mit Berücksichtigung von (1) und (3), das Resultat

$$n' = n + mv, \quad \text{also } n' \equiv n \,(\text{mod. } m).$$

Hieraus folgt, dass alle Wurzeln n der Congruenz (4), welche auf die obige Art aus einer gegebenen eigentlichen Darstellung (x, y) der Zahl m durch die Form (a, b, c) abgeleitet werden können, die sämmtlichen Individuen einer und derselben Zahlclasse (mod. m) sind, also nur eine und dieselbe Wurzel dieser Congruenz bilden (§. 21); jedes Individuum dieser Zahlclasse wird, wenn v alle ganzen Zahlen durchläuft, d. h. wenn man der Reihe nach alle Auflösungen ξ, η der Gleichung (2) betrachtet, ein Mal und auch nur ein Mal erzeugt. Man sagt daher, die Darstellung (x, y) der Zahl m *gehöre*

zu dieser Wurzel n (mod. m) der Congruenz (4), weil durch den angegebenen Process nur diese und keine andere Wurzel derselben zum Vorschein kommt.

Zugleich leuchtet ein, dass die Form (a, b, c) durch die sämmtlichen Substitutionen $\binom{x,\ \xi}{y,\ \eta}$, deren erster und dritter Coefficient die beiden darstellenden Zahlen x und y sind, in unendlich viele äquivalente Formen (m, n, l) übergeht (vergl. §. 56), deren gemeinschaftlicher erster Coefficient die dargestellte Zahl m ist, während der mittlere Coefficient n alle Zahlen einer völlig bestimmten Classe (mod. m), und zwar jedes Individuum derselben nur ein Mal, durchläuft *).

3. Das Vorhergehende reicht hin, um übersehen zu können, dass die *Aufgabe, alle eigentlichen Darstellungen einer gegebenen Zahl m durch eine gegebene Form (a, b, c) zu finden*, auf die Lösung der beiden Probleme zurückkommt, die wir am Schluss des vorigen Paragraphen aufgestellt haben. Man untersuche zunächst, ob D quadratischer Rest von m ist oder nicht; im letztern Fall

*) Es liegt nahe, die Zahlclasse n (mod. m) unmittelbar aus der gegebenen Darstellung (x, y) selbst zu bestimmen, ohne Zuziehung der Zahlen ξ, η. Die Auflösung der beiden Gleichungen (2) und (3), welche beide vom ersten Grade in Bezug auf ξ, η sind, giebt

$$m\eta = ax + (b+n)y, \quad -m\xi = (b-n)x + cy,$$

und hieraus folgen die Congruenzen

$$-yn \equiv ax + by, \quad xn \equiv bx + cy \text{ (mod. } m),$$

durch welche die Zahlclasse n (mod. m), wie man leicht erkennt, vollständig bestimmt ist. —

Wir schalten an dieser Stelle noch folgenden Satz ein, von welchem wir später Gebrauch machen werden: Giebt es zwei ganze Zahlen x, y, welche den Bedingungen

$$ax^2 + 2bxy + cy^2 = m$$

$$ax + (b+n)y \equiv 0, \quad (b-n)x + cy \equiv 0 \text{ (mod. } m)$$

genügen, wo m, n, a, b, c gegebene Zahlen bedeuten, deren erste von Null verschieden ist, so ist die Form (a, b, c) mit einer Form (m, n, l) äquivalent, deren erste beide Coefficienten m, n sind. Denn setzt man die auf der linken Seite der beiden Congruenzen befindlichen Ausdrücke resp. gleich $m\eta$, $-m\xi$, so ergiebt sich durch Multiplication mit x, y und Addition $m(x\eta - y\xi) = m$, also $x\eta - y\xi = +1$, woraus dann das Uebrige leicht folgt. Dass ferner umgekehrt, wenn zwei Formen (a, b, c) und (m, n, l) äquivalent sind, stets zwei Zahlen x, y existiren, welche den vorstehenden Bedingungen genügen, leuchtet aus dem Obigen unmittelbar ein. Mithin ist die Existenz zweier solcher Zahlen x, y vollkommen charakteristisch für die Aequivalenz der beiden Formen.

ist m durch keine einzige Form der Determinante D eigentlich darstellbar; im erstern Fall bestimme man alle incongruenten Wurzeln der Congruenz (4), und verfahre mit jeder einzelnen, wie folgt. Es sei n ein bestimmter Repräsentant einer bestimmten Wurzel, und zwar $n^2 = D + ml$, so ist (m, n, l) eine bestimmte Form von der Determinante D. Giebt es nun eine Darstellung (x, y) der Zahl m durch (a, b, c), welche zu der durch n repräsentirten Wurzel der Congruenz (4) gehört, so ist die Form (a, b, c) äquivalent mit (m, n, l), und die Darstellung (x, y) liefert eine und nur eine Substitution $\binom{x,\ \xi}{y,\ \eta}$, durch welche die erstere in die letztere übergeht. Es muss daher zunächst entschieden werden, ob die beiden gegebenen Formen (a, b, c) und (m, n, l) von der Determinante D äquivalent sind, oder nicht — dies ist das *erste* der beiden genannten Probleme; gesetzt nun, die beiden Formen erweisen sich als nicht äquivalent, so existirt keine einzige zu dieser Wurzel n gehörige Darstellung der Zahl m durch die Form (a, b, c). Zeigt es sich aber, dass die beiden Formen äquivalent sind, so müssen alle Substitutionen $\binom{x,\ \xi}{y,\ \eta}$ aufgesucht werden, durch welche (a, b, c) in (m, n, l) übergeht — dies ist das *zweite* Problem. Der erste und dritte Coefficient (x und y) einer jeden solchen Substitution bilden dann auch wirklich eine eigentliche zu der Wurzel n gehörige Darstellung der Zahl m durch (a, b, c), und da, wie schon bemerkt, aus jeder solchen Darstellung (x, y) umgekehrt eine und nur eine solche Substitution $\binom{x,\ \xi}{y,\ \eta}$ entspringt, so erhält man durch die sämmtlichen Substitutionen der angegebenen Art auch *alle* zu n gehörigen Darstellungen, und jede nur *ein Mal.* Genau in derselben Weise verfährt man mit den übrigen Wurzeln der Congruenz (4), deren Anzahl, falls m und D relative Primzahlen sind, nach §. 37 zu bestimmen ist.

§. 61.

Nachdem wir uns in der vorhergehenden Digression davon überzeugt haben, dass in der That die Theorie der Darstellung vollständig auf die beiden (in §. 59) erwähnten Probleme der Lehre von der Aequivalenz zurückgeführt werden kann, so wenden wir uns nun zu der Lösung derselben. Das *erste*, zu erkennen, ob zwei Formen von gleicher Determinante äquivalent sind oder nicht, erfordert von vorn herein ganz verschiedene Methoden, je nachdem

die Determinante *positiv* oder *negativ* ist; in beiden Fällen ist aber die Lösung von der Art, dass, wenn die Aequivalenz der beiden Formen erkannt wird, zu gleicher Zeit auch eine Transformation der einen in die andere gefunden wird. Da also bei zwei wirklich äquivalenten Formen immer eine solche Transformation durch die Lösung der ersten Aufgabe gefunden ist, so besteht das *zweite* Problem nur noch darin, aus *einer* solchen Transformation *alle anderen* zu finden; und da die Lösung desselben zunächst nicht von dem Vorzeichen der Determinante abhängt, sondern für positive wie für negative Determinanten Anfangs eine gleichmässige Behandlung zulässt, so stellen wir es dem andern voran.

Unsere Aufgabe ist also die, aus *einer* Substitution L, durch welche eine Form φ in eine äquivalente Form ψ übergeht, *alle* Substitutionen S zu finden, welche denselben Erfolg haben. Wir können dieselbe sogleich durch einige Bemerkungen bedeutend vereinfachen, indem wir sie auf den einfachsten Fall reduciren, in welchem beide Formen identisch sind. Denn gesetzt, wir kennen *alle* Substitutionen T, durch welche die Form φ in sich selbst übergeht, so geht φ offenbar durch alle Substitutionen TL in die andere Form ψ über. Alle diese Substitutionen TL gehören also zu den gesuchten Substitutionen S. Jetzt behaupten wir auch umgekehrt, dass auf diese Weise alle Substitutionen S erzeugt werden, und jede nur ein einziges Mal; denn bezeichnen wir mit L' die inverse Substitution von L (durch welche also die Form ψ in die Form φ zurückkehrt), so ist jede in der Form SL' enthaltene Substitution eine solche, durch welche die Form φ in sich selbst übergeht, und gehört mithin zu den mit T bezeichneten Substitutionen, so dass wir $SL' = T$ setzen können. Da nun die aus L' und L zusammengesetzte Substitution $L'L = \binom{1,\ 0}{0,\ 1}$ ist, so folgt hieraus $SL'L = S = TL$, also wird wirklich jede Substitution S auf die angegebene Art erzeugt. Dass endlich jede Substitution S nur ein einziges Mal erzeugt wird, leuchtet hieraus ebenfalls ein; ist nämlich $TL = S$, so ist $T = SL'$, also ist die Substitution T, durch welche eine bestimmte Substitution S erzeugt wird, immer eine vollkommen bestimmte, so dass zwei verschiedene Substitutionen T auch zwei verschiedene Substitutionen S erzeugen.

Da also der Complex der Substitutionen S vollständig mit dem Complex der Substitutionen TL übereinstimmt, wo L die gegebene Substitution bedeutet, durch welche die Form φ in die äquivalente Form ψ übergeht, so kommt es nur noch darauf an,

alle Substitutionen T zu finden; unser Problem ist daher auf das folgende zurückgeführt:

Alle Substitutionen zu finden, durch welche eine Form in sich selbst übergeht.

Bevor wir zur Lösung desselben schreiten, stellen wir eine Betrachtung an, welche für die Folge von grosser Wichtigkeit ist. Bedeutet σ den grössten (positiven) gemeinschaftlichen Theiler der drei Zahlen a, $2b$, c, so leuchtet ein, dass alle durch die Form (a, b, c) darstellbaren Zahlen durch σ theilbar sind, und wir wollen, wo kein Missverständniss zu besorgen ist, diese Zahl σ kurz *den Theiler der Form* (a, b, c) nennen. Dann sind zwei Fälle möglich:

1. Ist $2b : \sigma$ eine gerade Zahl, so geht σ in b, und folglich σ^2 in der Determinante $D = b^2 - ac$ auf; und umgekehrt, wenn σ^2 in D aufgeht, so ist b durch σ theilbar, also $2b : \sigma$ eine gerade Zahl; zugleich ist dann σ der grösste gemeinschaftliche Theiler der drei Coefficienten a, b, c.

2. Ist $2b : \sigma$ eine ungerade Zahl, so ist σ jedenfalls gerade, und σ^2 geht nicht in D, wohl aber in $4D$ auf, und zwar ist

$$\frac{4D}{\sigma^2} = \left(\frac{2b}{\sigma}\right)^2 - 4\frac{a}{\sigma}\frac{c}{\sigma} \equiv 1 \pmod{4},$$

also $4D \equiv \sigma^2 \pmod{4\sigma^2}$; und umgekehrt, wenn $4D \equiv \sigma^2 \pmod{4\sigma^2}$, so ist auch $(2b)^2 \equiv \sigma^2 \pmod{4\sigma^2}$, folglich $2b : \sigma$ eine ungerade Zahl; zugleich ist $\frac{1}{2}\sigma$ der grösste gemeinschaftliche Theiler der drei Coefficienten a, b, c.

Der Theiler σ einer jeden Form von der Determinante D genügt daher entweder der Bedingung $D \equiv 0 \pmod{\sigma^2}$, oder dieser $4D \equiv \sigma^2 \pmod{4\sigma^2}$; umgekehrt, ist σ eine positive Zahl, welche der einen oder andern dieser Bedingungen genügt, so existiren auch Formen (a, b, c) von der Determinante D, deren Theiler σ ist; je nachdem nämlich σ der ersten oder der zweiten Bedingung genügt, ist

$$\left(\sigma,\ 0,\ \frac{-D}{\sigma}\right) \quad \text{oder} \quad \left(\sigma,\ \tfrac{1}{2}\sigma,\ \frac{\sigma^2 - 4D}{4\sigma}\right)$$

eine Form von der Determinante D und vom Theiler σ, und zwar die sogenannte *einfachste* solche Form (*forma simplicissima*); die einfachste Form $(1, 0, -D)$ vom Theiler 1 heisst die *Hauptform* (*forma principalis*) der Determinante D*).

*) *Gauss: D. A.* artt. 231, 25.

Der grösste gemeinschaftliche Theiler τ der drei Coefficienten a, b, c einer Form (a, b, c) ist im ersten Fall $= \sigma$, im zweiten $= \frac{1}{2}\sigma$; ist nun $\tau = 1$, so heisst die Form eine *ursprüngliche* *) (*forma primitiva*), und zwar, wenn $\sigma = 1$ ist, eine Form der *ersten Art* **) (*forma proprie primitiva* oder *forma propria* nach *Gauss*), dagegen, wenn $\sigma = 2$ und also $D \equiv 1 \pmod{4}$ ist, eine Form der *zweiten Art* (*forma improprie primitiva* oder *forma impropria*). Ist ferner $\tau > 1$, und $a = \tau a'$, $b = \tau b'$, $c = \tau c'$, $b'b' - a'c' = D'$, $D = \tau^2 D'$, so heisst die Form (a, b, c) *abgeleitet* (*derivata*) aus der ursprünglichen Form (a', b', c') der Determinante D'.

Aus den Formeln der Transformation [§. 54, (2)] geht nun hervor, dass, wenn eine Form (a', b', c') unter einer Form (a, b, c) enthalten ist, jeder gemeinschaftliche Theiler der Zahlen a, $2b$, c auch gemeinschaftlicher Theiler der Zahlen a', $2b'$, c' sein muss, woraus unmittelbar folgt, dass je zwei äquivalente Formen denselben Theiler σ besitzen; mithin kommt dieser Theiler allen zu einer und derselben Classe gehörigen Formen gemeinschaftlich zu, und kann daher füglich *der Theiler der Formenclasse* genannt werden. Dasselbe gilt offenbar von dem grössten gemeinschaftlichen Theiler τ der Coefficienten a, b, c einer jeden zu einer bestimmten Classe gehörigen Form (a, b, c). Hiernach leuchtet von selbst ein, was unter der *einfachsten Classe vom Theiler* σ, unter der *Hauptclasse*, unter einer *ursprünglichen Classe der ersten oder zweiten Art*, oder unter einer *abgeleiteten Classe* zu verstehen ist. Endlich bildet der Inbegriff aller Formen von gleicher Determinante D und von gleichem Theiler σ eine sogenannte *Ordnung* ***) (*ordo*), und aus dem Vorhergehenden folgt, dass dieselbe der Complex aller *Classen* der Determinante D ist, welche den Theiler σ haben.

§. 62.

Es sei nun $\binom{\lambda, \mu}{\nu, \varrho}$ irgend eine Substitution, durch welche die Form (a, b, c) von der Determinante D und vom Theiler σ in sich selbst übergeht, so ist zunächst

$$\lambda\varrho - \mu\nu = 1 \tag{1}$$

*) *Gauss: D. A.* art. 226.

**) *Dirichlet*: *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres.* 2e partie. §. 7. Crelle's Journal XXI.

***) *Gauss: D. A.* art. 226.

und ferner (nach §. 54)

$$a\lambda^2 + 2b\lambda\nu + c\nu^2 = a; \qquad (2)$$

$$a\lambda\mu + b(\lambda\varrho + \mu\nu) + c\nu\varrho = b; \qquad (3)$$

da aus diesen drei Gleichungen schon folgt, dass (a, b, c) in eine äquivalente Form übergeht, deren erster und zweiter Coefficient a und b sind, so ist der letzte Coefficient c' der neuen Form wegen der Gleichheit der Determinanten nothwendig $= c$; und folglich drücken diese Gleichungen vollständig aus, dass $\binom{\lambda,\ \mu}{\nu,\ \varrho}$ eine Substitution der verlangten Art ist (dies würde nicht ebenso vollständig geschehen, wenn man die Gleichung $\lambda\varrho - \mu\nu = 1$ durch die andere Gleichung $a\mu^2 + 2b\mu\varrho + c\varrho^2 = c$ ersetzen wollte; denn dann würde man rückwärts nur schliessen können, dass $\lambda\varrho - \mu\nu = \pm 1$ ist).

Wir behandeln diese drei Gleichungen mit den vier Unbekannten λ, μ, ν, ϱ auf folgende Weise.

Wird $\lambda\varrho$ durch $\mu\nu + 1$ ersetzt, so nimmt die Gleichung (3) die Form

$$a\lambda\mu + 2b\mu\nu + c\nu\varrho = 0$$

an; verbindet man hiermit die Gleichung (2) und eliminirt einmal $2b$, dann c, so erhält man unter Berücksichtigung der Gleichung (1) die beiden folgenden:

$$a\mu + c\nu = 0; \quad a(\lambda - \varrho) + 2b\nu = 0.$$

Da a von Null verschieden ist (weil sonst D eine Quadratzahl wäre), so kann man folglich

$$\nu = \frac{a}{\sigma}u, \quad \mu = -\frac{c}{\sigma}u, \quad \lambda - \varrho = -\frac{2b}{\sigma}u \qquad (4)$$

setzen, worin u eine neue unbekannte, aber *ganze* Zahl bedeutet, weil ν, μ, $\lambda - \varrho$ ganze Zahlen sind, und σ der grösste gemeinschaftliche Divisor von a, c, $2b$ ist. Setzen wir diese Ausdrücke für μ und ν in die Gleichung (1), so erhalten wir

$$\lambda\varrho = -\frac{ac}{\sigma^2}u^2 + 1,$$

und hieraus in Verbindung mit dem vorstehenden Ausdruck für $\lambda - \varrho$ die Gleichung

$$(\lambda + \varrho)^2 = (\lambda - \varrho)^2 + 4\lambda\varrho = \frac{4(Du^2 + \sigma^2)}{\sigma^2}$$

oder

$$\left(\frac{\sigma(\lambda + \varrho)}{2}\right)^2 = Du^2 + \sigma^2.$$

Hieraus ergiebt sich, dass $\frac{1}{2}\sigma(\lambda+\varrho)$ jedenfalls eine *ganze* Zahl sein muss, die wir mit t bezeichnen wollen, so dass

$$\lambda+\varrho=\frac{2t}{\sigma} \text{ und } t^2=Du^2+\sigma^2 \tag{5}$$

ist.

Wir können die vorstehende Untersuchung mit Rücksicht auf (4) und (5) in Folgendem zusammenfassen*):

Ist $\binom{\lambda,\ \mu}{\nu,\ \varrho}$ *eine Substitution, durch welche die Form* (a, b, c) *von der Determinante* D *und vom Theiler* σ *in sich selbst übergeht, so ist stets*

$$\begin{aligned} \lambda &= \frac{t-bu}{\sigma}, & \mu &= -\frac{cu}{\sigma} \\ \nu &= \frac{au}{\sigma}, & \varrho &= \frac{t+bu}{\sigma} \end{aligned} \tag{I}$$

wo t, u *zwei ganze Zahlen bedeuten, welche der unbestimmten Gleichung*

$$t^2-Du^2=\sigma^2 \tag{II}$$

Genüge leisten.

Aber dieser Satz lässt sich auch umkehren:

Sind t, u *zwei ganze der Gleichung* (II) *genügende Zahlen, so sind die durch die Gleichungen* (I) *bestimmten Zahlen* $\lambda, \mu, \nu, \varrho$ *die ganzzahligen Coefficienten einer Substitution* $\binom{\lambda,\ \mu}{\nu,\ \varrho}$, *durch welche die Form* (a, b, c) *in sich selbst übergeht.*

Dies ergiebt sich auf folgende Weise. Zunächst ist zu beweisen, dass $\lambda, \mu, \nu, \varrho$ *ganze* Zahlen werden; da σ in a und in c aufgeht, so sind ν und μ ganze Zahlen; da ferner σ^2 in $4D$ und zufolge (II) auch in $4t^2$ aufgeht, so ist $2t$ theilbar durch σ, und da σ auch in $2b$ aufgeht, so sind 2λ und 2ϱ ebenfalls ganze Zahlen, deren Summe $= 4t:\sigma$, also eine gerade Zahl ist; mithin sind 2λ und 2ϱ entweder beide gerade oder beide ungerade; da aber ihr Product

$$=4\frac{t^2-b^2u^2}{\sigma^2}=4\frac{\sigma^2-acu^2}{\sigma^2}=4\left(1-\frac{a}{\sigma}\frac{c}{\sigma}u^2\right)$$

gerade ist, so sind 2λ und 2ϱ gerade Zahlen, also λ und ϱ ganze Zahlen.

Nachdem dieser erste Punct sichergestellt ist, findet man leicht durch wirkliche Substitution der Ausdrücke (I) unter Berücksichtigung der Gleichung (II), dass die drei Relationen (1),

*) Vergl. *Gauss*: *D. A.* art. 162.

(2) und (3) identisch erfüllt sind, dass also in der That die Form (a, b, c) durch die Substitution $\binom{\lambda, \mu}{\nu, \varrho}$ in sich selbst übergeht.

Aus jeder bekannten Substitution $\binom{\lambda, \mu}{\nu, \varrho}$ kann daher (z. B. durch die Gleichungen $u = \sigma\nu : a$, $t = \sigma\lambda + bu$) eine Auflösung t, u der Gleichung (II) gefunden werden, und umgekehrt. Es ist aber wichtig, zu bemerken, dass zwei verschiedenen Substitutionen auch zwei verschiedene Auflösungen der Gleichung (II) entsprechen, und umgekehrt zwei verschiedenen Auflösungen der Gleichung (II) auch zwei verschiedene Transformationen der Form (a, b, c) in sich selbst. Denn die Relationen (I) sind derartig, dass gegebenen Werthen t, u ein und nur ein System von Werthen λ, μ, ν, ϱ, und umgekehrt gegebenen Werthen von $\lambda, \mu, \nu, \varrho$ ein und nur ein System von Werthen t, u entspricht.

Hiermit ist also unser Problem nicht vollständig gelöst, sondern nur auf das andere reducirt:

Alle ganzzahligen Auflösungen der unbestimmten Gleichung (II) *zu finden.*

Dieses letztere bietet nun nicht die geringste Schwierigkeit dar, sobald die Determinante D *negativ* ist. Wenn nämlich Δ ihr absoluter Werth, also $D = -\Delta$ ist, so hat die Gleichung (II)

$$t^2 + \Delta u^2 = \sigma^2$$

nur eine *endliche* Anzahl von Auflösungen t, u; und zwar ist, wenn

1. $D \equiv 0 \pmod{\sigma^2}$, die Anzahl der Auflösungen der Gleichung immer $= 2$, sobald $\Delta > \sigma^2$ ist; diese Auflösungen sind offenbar

$$t = +\sigma, \quad u = 0 \quad \text{und} \quad t = -\sigma, \quad u = 0;$$

im Fall $\Delta = \sigma^2$ ist aber die Anzahl der Auflösungen $= 4$; diese sind

$$t = \sigma, \quad u = 0; \quad t = -\sigma, \quad u = 0;$$
$$t = 0, \quad u = 1; \quad t = 0, \quad u = -1.$$

2. Ist $4D \equiv \sigma^2 \pmod{4\sigma^2}$ und folglich $4\Delta \equiv 3\sigma^2 \pmod{4\sigma^2}$, so ist die Anzahl der Auflösungen der Gleichung stets $= 2$, so oft $4\Delta > 3\sigma^2$, also $4\Delta \geqq 7\sigma^2$; diese sind

$$t = \sigma, \quad u = 0; \quad \text{und} \quad t = -\sigma, \quad u = 0;$$

im Fall $4\Delta = 3\sigma^2$ ist aber die Anzahl der Auflösungen $= 6$; diese sind

$$t = +\sigma,\ u = 0; \quad t = +\tfrac{1}{2}\sigma,\ u = +1; \quad t = +\tfrac{1}{2}\sigma,\ u = -1;$$
$$t = -\sigma,\ u = 0; \quad t = -\tfrac{1}{2}\sigma,\ u = -1; \quad t = -\tfrac{1}{2}\sigma,\ u = +1.$$

§. 63.

Bei weitem schwieriger ist die Theorie der Gleichung (II) für den Fall einer *positiven* Determinante D, und hierin zeigt sich zuerst die grosse Verschiedenheit in der Natur der Formen von positiver und derer von negativer Determinante. Wir lassen daher diese Untersuchung für jetzt fallen, um sie später (in §. 83) wieder aufzunehmen, nachdem das andere in §. 59 erwähnte Problem der Lehre von der Aequivalenz seine Lösung gefunden haben wird. Auch bei diesem stellt sich etwas Aehnliches heraus, indem es durchaus nothwendig wird, die Formen von positiver und negativer Determinante vollständig gesondert zu behandeln; und da auch hier die Formen von negativer Determinante weit weniger Schwierigkeiten darbieten, so behandeln wir diese zunächst.

Um aber den Gang der Untersuchung nicht zu unterbrechen, schicken wir eine Bemerkung voraus, welche sich gleichmässig auf Formen von positiver wie von negativer Determinante bezieht. Offenbar geht eine Form (a, b, a'), in welcher wir absichtlich den letzten Coefficienten nicht mit c, sondern mit a' bezeichnen, durch eine Substitution von der Form $\left(\begin{smallmatrix}0, & 1\\ -1, & \delta\end{smallmatrix}\right)$ in eine äquivalente Form über, deren Coefficienten

$$a',\quad b' = -b - a'\delta,\quad a'' = a + 2b\delta + a'\delta^2$$

sind; diese Form (a', b', a'') soll der Form (a, b, a') *nach rechts benachbart**), und ebenso soll die letztere (a, b, a') der andern (a', b', a'') *nach links benachbart* heissen. Das Charakteristische der Beziehung zweier solcher benachbarter Formen φ und φ' (*formae contiguae*) besteht *erstens* darin, dass sie dieselbe Determinante haben, *zweitens*, dass der letzte Coefficient a' der einen Form φ zugleich der erste Coefficient der andern Form φ' ist, *drittens*, dass die Summe ihrer mittlern Coefficienten $b + b'$ durch diesen gemeinschaftlichen Coefficienten a' theilbar ist. Denn haben zwei Formen φ und φ' diese drei Eigenschaften, und setzt man $b + b' = -a'\delta$, so geht in der That die Form φ durch die Substitution

$$\begin{pmatrix}0, & 1\\ -1, & \delta\end{pmatrix}$$

*) *Gauss: D. A.* art. 160.

in eine neue Form über, deren erste beide Coefficienten a', b' mit denen der Form φ' übereinstimmen; und da die neue Form jedenfalls der Form φ äquivalent ist, also auch dieselbe Determinante wie φ und folglich auch wie φ' hat, so muss sie mit φ' identisch sein *).

§. 64.

Wir wenden uns nun zu der Untersuchung, ob zwei gegebene Formen von gleicher *negativer* Determinante $D = -\Delta$ äquivalent sind oder nicht. Zunächst ist zu bemerken, dass die beiden äusseren Coefficienten a und c einer solchen Form

$$\varphi = ax^2 + 2bxy + cy^2$$

nothwendig gleiche Vorzeichen haben, da $ac = b^2 + \Delta$ positiv ist; da ferner

$$a\varphi = (ax + by)^2 + \Delta y^2$$

ist, so zeigt sich, dass alle durch die Form φ darstellbaren Zahlen dasselbe Vorzeichen haben wie a und c. Sind daher (a, b, c) und (a', b', c') äquivalente Formen, so haben die äusseren Coefficienten a', c' der letztern Form dasselbe Zeichen wie die der erstern. Da ferner aus der Aequivalenz dieser beiden Formen auch die der beiden Formen $(-a, -b, -c)$ und $(-a', -b', -c')$ folgt, so können wir uns im Folgenden auf die Betrachtung der sogenannten *positiven* Formen beschränken, in welchen die beiden äusseren Coefficienten das *positive* Vorzeichen haben.

Um nun über die Aequivalenz zweier Formen dieser Art zu entscheiden, vergleicht man sie nicht direct mit einander, sondern

---

*) Der letzte Grund, weshalb die Substitutionen von der Form $\binom{0,\ 1}{-1,\ \delta}$ eine so wichtige Rolle spielen, besteht darin, dass aus ihnen alle anderen sich zusammensetzen lassen; man kann die Coefficienten δ in ihrer Aufeinanderfolge noch gewissen Beschränkungen, namentlich in Bezug auf ihre Vorzeichen, unterwerfen, in der Art, dass jede beliebige Substitution sich auch nur auf eine einzige Weise aus solchen einfachen Substitutionen zusammensetzen lässt. Eine wichtige Anwendung findet diese Bemerkung z. B. in der Theorie der unendlich vielen Formen der ϑ-Functionen. Man erkennt ferner leicht, dass auch der in §. 23 behandelte Algorithmus in der Theorie dieser Substitutionen und ihrer Zusammensetzung enthalten ist. Man vergleiche ferner §. 81.

mit sogenannten *reducirten**) Formen. Man nennt eine Form (A, B, C) von negativer Determinante (und positiven äusseren Coefficienten) eine reducirte, wenn der letzte Coefficient C nicht kleiner ist als der erste A, und der erste A wieder nicht kleiner als der absolute Werth des doppelten mittlern Coefficienten $2B$, in Zeichen, wenn

$$C \geqq A \geqq 2(B)$$

ist, wo (B) den absoluten Werth von B bedeuten soll. Wir beweisen nun zunächst folgenden Satz:

Jede Form von negativer Determinante ist einer reducirten Form äquivalent.

Zu dem Zweck betrachte man die der gegebenen Form (a, b, a') nach rechts benachbarten Formen (a', b', a''); unter diesen wird es immer eine (bisweilen auch zwei) geben, in welchen wenigstens die eine Bedingung $a' \geqq 2(b')$ erfüllt ist. Denn unter allen mit $-b$ nach dem Modul a' congruenten Zahlen giebt es eine b', deren absoluter Werth am kleinsten, und zwar kleiner oder wenigstens nicht grösser als $\frac{1}{2}a'$ ist (falls a' gerade und $b \equiv \frac{1}{2}a'$ (mod. a') ist, würde es zwei solche Zahlen b' geben, nämlich $\pm \frac{1}{2}a'$), so dass jedenfalls $b' \equiv -b$ (mod. a') und ausserdem $2(b') \leqq a'$ ist. Ist b' auf diese Weise gefunden, und $b + b' = -a'\delta$, so geht die Form (a, b, a') durch die Substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

in die nach rechts benachbarte Form (a', b', a'') über, in welcher $2(b') \leqq a'$ ist. Wenn nun gleichzeitig sich herausstellt, dass $a' \leqq a''$ ist, so ist (a', b', a'') eine reducirte Form und der Process geschlossen. Findet sich aber, dass das Gegentheil

$$a' > a''$$

Statt findet, so ist (a', b', a'') noch keine reducirte Form. Mit dieser verfahre man ebenso wie mit (a, b, a'), d. h. man transformire sie in eine nach rechts benachbarte Form (a'', b'', a'''), in welcher $2(b'') \leqq a''$ ist; sobald dann gleichzeitig $a'' \leqq a'''$ ist, so ist (a'', b'', a''') reducirt, folglich der Process geschlossen; ist dies aber nicht der Fall, also

$$a'' > a''',$$

*) *Gauss: D. A.* art. 171. Die Bedingung $A \leqq \sqrt{\frac{4}{3}\Delta}$ ist schon eine Folge der beiden anderen (vergl. §. 65).

so setze man den Process in derselben Weise fort. Immer aber wird er nach einer *endlichen* Anzahl von Operationen schliessen; denn wäre dies nicht der Fall, so hätte man eine nie abbrechende Reihe von positiven ganzen Zahlen

$$a', a'', a''' \ldots a^{(n)}, a^{(n+1)} \ldots,$$

in welcher jede folgende mindestens um eine Einheit kleiner wäre, als die unmittelbar vorausgehende, was unmöglich ist, da es immer nur eine endliche Anzahl ganzer positiver Zahlen giebt, welche kleiner sind als eine gegebene.

Auf diese Weise ist bewiesen, dass man endlich zu einer Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ gelangen muss, in welcher nicht nur $2(b^{(n)}) \leqq a^{(n)}$, sondern auch $a^{(n)} \leqq a^{(n+1)}$ ist.

Zugleich ergiebt sich jedesmal durch die wirkliche Ausführung der Operationen eine Substitution, welche aus den successiven Substitutionen von der Form

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

zusammengesetzt ist, und durch welche die gegebene Form (a, b, a') in die ihr äquivalente reducirte Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ übergeht.

Nehmen wir als Beispiel die Form (200, 100, 51), deren Determinante $D = -200$ ist, so haben wir $b' \equiv -100 \pmod{51}$ zu setzen und finden hieraus $b' = 2$ und $\delta = -2$; die Substitution, durch welche die gegebene Form (200, 100, 51) transformirt werden muss, ist daher gefunden; da wir aber den ersten und zweiten Coefficienten a' und b' und die Determinante D kennen, so brauchen wir diese Transformation nicht wirklich auszuführen, sondern wir berechnen den letzten Coefficienten a'' durch die Formel

$$a'' = \frac{b'^2 - D}{a'} = a + (b - b')\delta;$$

in unserm Fall finden wir also $a'' = 4$. Die benachbarte Form ist daher (51, 2, 4); sie ist nicht reducirt, weil der letzte Coefficient kleiner ist als der erste. Wir wiederholen daher dieselbe Operation, indem wir $b'' \equiv -2 \pmod{4}$ und folglich $b'' = \pm 2$ setzen, wo beide Zeichen zulässig sind; dann ergiebt sich $\delta' = -1$ oder $= 0$, je nachdem das obere oder untere Zeichen genommen wird, und ausserdem $a''' = 51$; also ist die neue Form $(4, \pm 2, 51)$, und diese ist, mag man das obere oder das untere Zeichen wählen, reducirt. Ferner geht die gegebene Form (200, 100, 51) durch die Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & -2 \end{pmatrix} \begin{pmatrix} 0, & +1 \\ -1, & -1 \end{pmatrix} = \begin{pmatrix} -1, & -1 \\ +2, & +1 \end{pmatrix}$$

in die Form (4, 2, 51), dagegen durch die Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & -2 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} -1, & +0 \\ +2, & -1 \end{pmatrix}$$

in die Form (4, —2, 51) über. Man sieht aus diesem Beispiele wie einfach der angegebene Algorithmus sich gestaltet.

§. 65.

Wir sehen ferner an dem eben behandelten Beispiele, dass eine und dieselbe Form zwei verschiedenen reducirten Formen äquivalent sein kann, woraus folgt, dass auch zwei verschiedene reducirte Formen unter einander äquivalent sein, also derselben Classe angehören können. Da es von grosser Wichtigkeit ist, dies allgemein zu untersuchen, so stellen wir uns die Frage:

Wann sind zwei reducirte Formen (a, b, c) und (a', b', c') von gleicher negativer Determinante $D = -\Delta$ einander äquivalent?

Zunächst ziehen wir einige Folgerungen aus den beiden Bedingungen

$$2(b) \leqq a, \quad a \leqq c,$$

welche ausdrücken, dass die Form (a, b, c) eine reducirte ist. Es ergiebt sich nämlich aus der erstern $4b^2 \leqq a^2$, aus der letztern $a^2 \leqq ac$, also auch $4b^2 \leqq ac$ oder $3b^2 \leqq ac - b^2$, folglich

$$(b) \leqq \sqrt{\tfrac{1}{3}\Delta}.$$

Hieraus folgt weiter, dass $3ac = 3\Delta + 3b^2 \leqq 4\Delta$ und, da $a^2 \leqq ac$ ist, dass

$$a \leqq \sqrt{\tfrac{4}{3}\Delta}$$

ist.

Nehmen wir jetzt an, die beiden reducirten Formen (a, b, c), (a', b', c') seien äquivalent, so dürfen wir, ohne die Allgemeinheit zu beeinträchtigen, voraussetzen, dass

$$a' \leqq a$$

ist. Es sei nun $\binom{\alpha, \beta}{\gamma, \delta}$ die Substitution, durch welche (a, b, c) in (a', b', c') übergeht, also

$$1 = \alpha\delta - \beta\gamma \qquad (1)$$

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \qquad (2)$$

$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta. \qquad (3)$$

Multipliciren wir die Gleichung (2) mit a, so ergiebt sich

$$aa' = (a\alpha + b\gamma)^2 + \Delta\gamma^2;$$

da nun sowohl a, als auch $a' \leqq \sqrt{\frac{4}{3}\Delta}$, und also

$$aa' \leqq \tfrac{4}{3}\Delta$$

ist, so folgt, dass in der vorstehenden Gleichung γ^2 entweder $= 0$ oder $= 1$ sein muss; denn wäre $\gamma^2 \geqq 4$, so wäre $aa' \geqq 4\,\Delta$, was mit der Bedingung $aa' \leqq \frac{4}{3}\Delta$ streitet. Wir unterscheiden nun diese beiden Fälle:

I. $\gamma = 0$.

Dann lauten die drei obigen Gleichungen folgendermaassen:

$$\alpha\delta = 1;\ a' = a\alpha^2;\ b' = a\alpha\beta + b;$$

aus der ersten folgt $\alpha = \delta = \pm 1$; also ist $a' = a$, und die dritte Gleichung lehrt, dass $b' - b = \pm\, a\beta$ durch $a = a'$ theilbar ist; da nun aber $(b) \leqq \frac{1}{2}a$ und $(b') \leqq \frac{1}{2}a'$, also auch $(b') \leqq \frac{1}{2}a$ ist, so sind nur zwei Fälle möglich: entweder ist $b' - b = 0$, also $b' = b$ und folglich, da schon $a' = a$ ist, auch $c' = c$, d. h. die Formen sind identisch, in welchem Fall sich die Aequivalenz von selbst versteht; oder es ist der absolute Werth von $b' - b$, da er unmöglich grösser als a sein kann und doch durch a theilbar sein muss, gleich a; in diesem Fall muss eine der beiden Zahlen b, b' gleich $+\frac{1}{2}a$, die andere gleich $-\frac{1}{2}a$, und also $c' = c$ sein; wir werden daher auf zwei nicht identische ambige Formen $(a, \frac{1}{2}a, c)$ und $(a, -\frac{1}{2}a, c)$ geführt. Diese sind aber in der That äquivalent, und die erstere geht in die letztere durch die Substitution $\binom{1,\ -1}{0,\ +1}$ über.

II. $\gamma = \pm 1$.

In diesem Fall lautet die Gleichung (2) folgendermaassen

$$a' = a\alpha^2 \pm 2b\alpha + c;$$

da wir angenommen haben, dass a' nicht grösser als a, und folglich auch nicht grösser als c ist, so folgt, dass

$$a\alpha^2 \pm 2b\alpha \leqq 0$$

ist. Da nun andererseits $2(b) \leqq a$ und stets $(\alpha) \leqq \alpha^2$, also auch der absolute Werth von $2b\alpha$ nicht grösser ist als $a\alpha^2$, so ist ganz gewiss

$$a\alpha^2 \pm 2b\alpha \geqq 0.$$

Es kann also $a\alpha^2 \pm 2b\alpha$ weder positiv noch negativ sein, und folglich ist

$$a\alpha^2 \pm 2b\alpha = 0,$$

also $a' = c$; da aber $a' \leqq a$ und $a \leqq c$, so folgt weiter, dass sowohl $a' = a$, als auch $c = a$ ist. Nun kann man die Gleichung (3) mit Hülfe der Gleichung (1) in die Form

$$b + b' = a\alpha\beta + 2b\alpha\delta \pm c\delta$$

bringen, und da $c = a$, und $2b\alpha = \mp a\alpha^2$ ist, so ergiebt sich

$$b + b' = a(\alpha\beta \mp \alpha^2\delta \pm \delta)$$

d. h. $b + b'$ ist theilbar durch a. Hieraus folgt ganz ähnlich wie im Fall I, dass $b + b'$ entweder $= 0$, oder dass der absolute Werth von $b + b'$ gleich a sein muss. Im letztern Fall müssten b und b' einander gleich, nämlich $= \pm \frac{1}{2}a$ sein, dann erhielte man also wieder den Fall zweier identischen Formen, der kein Interesse darbietet. Im erstern Fall dagegen ist $b' = -b$, folglich da $a' = a$, und auch $c = a$ ist, auch $c' = c = a$; wir haben daher folgende zwei Formen (a, b, a) und $(a, -b, a)$, welche (wenn b von Null verschieden ist) nicht identisch sind; diese sind wirklich äquivalent, und die erstere geht in die letztere durch die Substitution $\binom{0,\ -1}{1,\ \ 0}$ über.

Wir fassen das Resultat der Untersuchung in Folgendem zusammen:

Die beiden einzigen Fälle, in denen zwei nicht identische reducirte Formen derselben Classe angehören, sind die folgenden: die Formen $(a, \frac{1}{2}a, c)$ *und* (a, b, a) *gehen resp. durch die Substitutionen*

$$\begin{pmatrix}1, & -1\\ 0, & +1\end{pmatrix} \text{ und } \begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$$

in die entgegengesetzten Formen $(a, -\frac{1}{2}a, c)$ *und* $(a, -b, a)$ *über.*

§. 66.

Hiermit ist nun auch die Aufgabe gelöst, zu entscheiden, ob zwei Formen von gleicher negativer Determinante äquivalent sind oder nicht. Sind φ und ψ die beiden Formen, so transformire man jede derselben, falls sie noch nicht reducirt sein sollte, nach

der oben (§. 64) angegebenen Methode in eine reducirte Form, φ in φ', ψ in ψ'. Stellt sich dann heraus, dass φ' und ψ' identisch ausfallen, oder dass sie einen der beiden eben untersuchten Fälle darbieten, in welchen zwei nicht identische reducirte Formen dennoch äquivalent sind (was durch den Anblick der beiden Formen augenblicklich erkannt wird), so sind die gegebenen Formen φ und ψ gewiss äquivalent. Und zugleich ergiebt sich eine Substitution, durch welche die eine Form in die andere übergeht; denn durch den Process der Reduction ergeben sich Substitutionen S, durch welche φ in φ', und T, durch welche ψ in ψ' übergeht. Sind daher φ' und ψ' identisch, so geht, wenn T' die inverse Substitution von T bedeutet, die Form φ durch die zusammengesetzte Substitution ST' in die Form ψ über. Sind dagegen φ' und ψ' nicht identisch, aber doch äquivalent, so ist, wie wir oben gesehen haben, immer eine Substitution U bekannt, durch welche φ' in ψ' übergeht; und dann geht φ durch die zusammengesetzte Substitution SUT' in ψ über.

Zeigt sich aber, dass die Formen φ' und ψ' nicht identisch sind, und dass sie auch keinen der beiden im vorigen Paragraphen erwähnten singulären Fälle darbieten, sind also diese beiden reducirten Formen nicht äquivalent, so sind auch die beiden gegebenen Formen φ und ψ nicht äquivalent, wie unmittelbar aus §. 59 folgt.

Hiermit sind für negative Determinanten die beiden in §. 59 aufgestellten Probleme der Lehre von der Aequivalenz vollständig gelöst: soeben das erstere, welches darin besteht, über die Aequivalenz oder Nichtäquivalenz zweier gegebenen Formen zu entscheiden; und zugleich haben wir jedesmal, wenn die Entscheidung für die erstere lautet, auch eine Substitution zu finden gelehrt, durch welche die eine Form in die andere übergeht. Das zweite Problem, aus einer gegebenen Substitution, durch welche eine gegebene Form in eine (hierdurch schon völlig bestimmte) äquivalente Form übergeht, alle Substitutionen zu finden, durch welche die erstere Form in dieselbe zweite Form übergeht, ist in den §§. 61, 62 ebenfalls vollständig gelöst.

§. 67.

Die Theorie der reducirten Formen setzt uns nun auch in den Stand, für jede gegebene *negative* Determinante ein *vollständiges System nicht-äquivalenter Formen* (§. 59) aufzustellen, wobei wir uns wieder auf solche Formen beschränken wollen, deren äussere Coefficienten positiv sind. Da nämlich jede Form von negativer Determinante $D = -\Delta$ einer reducirten Form und im Allgemeinen auch nur einer solchen reducirten Form äquivalent ist, so brauchen wir, um ein vollständiges Formensystem zu erhalten, nur die sämmtlichen reducirten Formen aufzusuchen und jedesmal, wenn zwei solche nicht identische Formen einen der beiden in §. 65 erwähnten Fälle darbieten, eine von ihnen nach Belieben fortzulassen, die andere beizubehalten. Dass die Anzahl der so übrig bleibenden nicht äquivalenten reducirten Formen endlich ist, ergiebt sich leicht aus den Bedingungen

$$2(b) \leqq a \leqq c,$$

denen eine reducirte Form (a, b, c) genügen muss, und der hieraus (in §. 65) gezogenen Folgerung

$$(b) \leqq \sqrt{\tfrac{1}{3}\Delta}.$$

Bezeichnet man nämlich die grösste ganze in $\sqrt{\frac{1}{3}\Delta}$ enthaltene Zahl mit λ (so dass $\lambda \leqq \sqrt{\frac{1}{3}\Delta} < \lambda + 1$), so kann der mittlere Coefficient b keine andern, als die folgenden $2\lambda + 1$ Werthe

$$0, \ \pm 1, \ \pm 2 \ldots \pm \lambda$$

haben; und wenn man dem mittlern Coefficienten b irgend einen dieser Werthe beigelegt hat, so ist $ac = b^2 + \Delta$; also hat man die Zahl $b^2 + \Delta$ auf alle mögliche Arten in zwei positive Factoren zu zerlegen, und jedesmal denjenigen, welcher den andern an Grösse nicht übertrifft, für a, den letztern für c zu nehmen; stellt sich dann gleichzeitig heraus, dass $2(b) \leqq a$ ist, so ist die so gebildete Form wirklich eine reducirte und deshalb aufzuschreiben, im entgegengesetzten Fall aber fortzulassen. Auf diese Weise erhält man nothwendig alle reducirten Formen; ihre Anzahl ist aber nothwendig eine endliche, denn die Anzahl aller Zerlegungen der $(2\lambda + 1)$ Zahlen von der Form $(b^2 + \Delta)$ in zwei Factoren ist selbst endlich. Wir haben daher das Resultat:

Die Anzahl aller nicht äquivalenten reducirten Formen von negativer Determinante, d. h. die Classenanzahl selbst ist endlich.

Beispiel 1: Für die Determinante $D = -12$ ist $\Delta = 12$; hieraus $\lambda = \sqrt{\frac{1}{3}\Delta} = 2$; wir haben daher b folgende Werthe durchlaufen zu lassen

$$0, \ \pm 1, \ \pm 2,$$

und dann die Zahlen $b^2 + \Delta$, d. h. die Zahlen

$$12, \ 13, \ 16$$

auf alle möglichen Arten in zwei Factoren zu zerlegen; es ist

$$12 = 1 \,.\, 12 = 2 \,.\, 6 = 3 \,.\, 4$$
$$13 = 1 \,.\, 13$$
$$16 = 1 \,.\, 16 = 2 \,.\, 8 = 4 \,.\, 4.$$

Dies giebt, indem der erste Factor immer $= a$, der zweite $= c$ gesetzt wird, die eilf Formen

$$(1, 0, 12), \quad (2, 0, 6), \quad (3, 0, 4);$$
$$(1, \pm 1, 13);$$
$$(1, \pm 2, 16), \quad (2, \pm 2, 8), \quad (4, \pm 2, 4).$$

Von diesen sind die folgenden nicht reducirt

$$(1, \pm 1, 13), \quad (1, \pm 2, 16), \quad (2, \pm 2, 8),$$

weil in ihnen die Bedingung $2(b) \leqq a$ nicht erfüllt ist; als wirklich reducirte Formen bleiben daher nur die folgenden fünf übrig

$$(1, 0, 12), \quad (2, 0, 6), \quad (3, 0, 4), \quad (4, \pm 2, 4);$$

allein die beiden Formen $(4, 2, 4)$ und $(4, -2, 4)$ gehören unter die Ausnahmefälle des §. 65, sind also äquivalent. Mithin enthält das vollständige Formensystem nur *vier* Formen, nämlich

$$(1, 0, 12), \quad (2, 0, 6), \quad (3, 0, 4), \quad (4, 2, 4),$$

die als Repräsentanten ebenso vieler Classen gelten. Von diesen vier Formen sind nur die beiden folgenden

$$(1, 0, 12), \quad (3, 0, 4)$$

ursprünglich, und zwar sind (da D nicht $\equiv 1 \pmod{4}$ ist) beide von der ersten Art.

Beispiel 2: Ist $D = -35$, also $\Delta = +35$, so ist $\lambda = 3$ also kann b nur die sieben Werthe

$$0, \ \pm 1, \ \pm 2, \ \pm 3$$

durchlaufen; diesen entsprechen die Zahlen $b^2 + \Delta$:

35, 36, 39, 44;

die Zerlegungen derselben in zwei Factoren sind folgende:

$$35 = 1 . 35 = 5 . 7$$
$$36 = 1 . 36 = 2 . 18 = 3 . 12 = 4 . 9 = 6 . 6$$
$$39 = 1 . 39 = 3 . 13$$
$$44 = 1 . 44 = 2 . 22 = 4 . 11.$$

Aber von den 22 entsprechenden Formen erfüllen nur die folgenden 10 die Bedingung $2(b) \leqq a$:

$$(1, 0, 35), \quad (5, 0, 7), \quad (2, \pm 1, 18)$$
$$(3, \pm 1, 12), \quad (4, \pm 1, 9), \quad (6, \pm 1, 6).$$

Da ferner die beiden Formen $(2, \pm 1, 18)$ den Fall I, die beiden Formen $(6, \pm 1, 6)$ den Fall II des §. 64 darbieten, so existiren nur *acht* nicht äquivalente reducirte Formen

$$(1, 0, 35), \quad (5, 0, 7), \quad (2, 1, 18)$$
$$(3, \pm 1, 12), \quad (4, \pm 1, 9), \quad (6, 1, 6);$$

diese sind alle ursprünglich; sechs, nämlich

$$(1, 0, 35), \quad (5, 0, 7), \quad (3, \pm 1, 12), \quad (4, \pm 1, 9)$$

sind von der ersten, die beiden andern

$$(2, 1, 18), \quad (6, 1, 6)$$

sind von der zweiten Art.

Beispiel 3: Ist $D = -48 = -\Delta$, so ist $\lambda = 4$, so dass b folgende Zahlen

$$0, \pm 1, \pm 2, \pm 3, \pm 4$$

durchlaufen muss; die Zerlegungen der entsprechenden Zahlen $b^2 + \Delta$ sind folgende:

$$48 = 1 . 48 = 2 . 24 = 3 . 16 = 4 . 12 = 6 . 8$$
$$49 = 1 . 49 = 7 . 7$$
$$52 = 1 . 52 = 2 . 26 = 4 . 13$$
$$57 = 1 . 57 = 3 . 19$$
$$64 = 1 . 64 = 2 . 32 = 4 . 16 = 8 . 8.$$

Von den entsprechenden 27 Formen sind nur folgende eilf reducirt:

$$(1, 0, 48), \quad (2, 0, 24), \quad (3, 0, 16), \quad (4, 0, 12),$$
$$(6, 0, 8), \quad (7, \pm 1, 7), \quad (4, \pm 2, 13), \quad (8, \pm 4, 8).$$

Unter diesen besteht jedes der drei Paare $(7, \pm 1, 7)$, $(4, \pm 2, 13)$,

(8, ± 4, 8) aus je zwei äquivalenten Formen; also bleiben nur *acht* nicht äquivalente Formen

$$(1, 0, 48),\quad (2, 0, 24),\quad (3, 0, 16),\quad (4, 0, 12),$$
$$(6, 0, 8),\quad (7, 1, 7),\quad (4, 2, 13),\quad (8, 4, 8).$$

Ursprünglich von der ersten Art sind die folgenden vier:

$$(1, 0, 48),\quad (3, 0, 16),\quad (7, 1, 7),\quad (4, 2, 13),$$

die anderen vier sind derivirte Formen.

§. 68.

Um schon jetzt einen Begriff von der Fruchtbarkeit dieser Untersuchungen zu geben, verbinden wir in einigen Beispielen die gewonnenen Resultate mit der in §. 60 vorausgeschickten Theorie der Darstellung der Zahlen durch bestimmte quadratische Formen, bemerken jedoch gleich, dass die folgenden Sätze nur specielle Fälle eines grossen allgemeinen Satzes sind.

Die Formen der Determinante $D = -1$ bilden nur eine einzige Classe, denn es giebt für diese Determinante, wie man leicht erkennt, nur die einzige reducirte Form

$$(1, 0, 1) = x^2 + y^2.$$

Wir fragen nun nach dem System der durch diese Form darstellbaren, d. h. also in zwei Quadrate zerlegbaren Zahlen m; um aber die frühere Theorie unmittelbar anwenden zu können, lassen wir nur *eigentliche* Darstellungen (x, y) gelten, in denen die beiden darstellenden Zahlen x, y relative Primzahlen sind; ferner wollen wir uns der Einfachheit halber auf *ungerade* darstellbare Zahlen m beschränken. Es sei also m eine solche darstellbare ungerade Zahl, so ist zunächst m positiv. Da ferner die Determinante -1 quadratischer Rest von m ist, so müssen alle in m aufgehenden Primzahlen von der Form $4h + 1$ sein. Umgekehrt, ist diese Bedingung erfüllt, so ist die Determinante -1 quadratischer Rest von m, und die Congruenz

$$z^2 \equiv -1 \pmod{m}$$

hat im Ganzen (nach §. 37) 2^μ incongruente Wurzeln, wenn μ die Anzahl dieser von einander verschiedenen in m aufgehenden Primzahlen bedeutet (dies gilt selbst für den Fall, in welchem $\mu = 0$,

$m=1$ ist). Es sei n ein bestimmter Repräsentant einer bestimmten dieser Wurzeln, und $n^2+1=ml$, so bilde man die quadratische Form (m, n, l) von der Determinante -1; da nur eine einzige Formenclasse existirt, so ist diese Form der reducirten Form $(1, 0, 1)$ nothwendig äquivalent, und man wird durch die in §. 66 angegebene Methode eine, und hieraus nach §§. 61, 62 alle Transformationen finden, durch welche $(1, 0, 1)$ in (m, n, l) übergeht. Die Anzahl dieser von einander verschiedenen Transformationen $\binom{x,\ \xi}{y,\ \eta}$ ist (nach §§. 61, 62) stets $=4$; ebenso viele Darstellungen (x, y) der Zahl m existiren daher, welche zu derjenigen Wurzel gehören, deren Repräsentant n ist. Und da dasselbe Raisonnement auf jede der 2^μ Wurzeln der obigen Congruenz passt, so existiren im Ganzen

$$4 \cdot 2^\mu = 2^{\mu+2}$$

verschiedene Darstellungen der Zahl m.

Stellt man aber die Frage, auf wie viele verschiedene Arten eine solche Zahl m in zwei Quadrate zerlegt werden kann, ohne Rücksicht auf die Ordnung der beiden Quadrate und auf die Vorzeichen ihrer Wurzeln, so liefern je acht verschiedene Darstellungen von der Form

$$(\pm x, \pm y) \text{ und } (\pm y, \pm x)$$

nur eine einzige Zerlegung $m = x^2 + y^2$ (von diesen acht Darstellungen gehören vier, nämlich

$$(x, y), (-x, -y), (-y, x), (y, -x)$$

zu einer, und die anderen vier

$$(x, -y), (-x, y), (-y, -x), (y, x)$$

zu der ihr entgegengesetzten Wurzel); folglich ist die Anzahl dieser verschiedenen Zerlegungen

$$= 2^{\mu-1},$$

mit einziger Ausnahme des Falles $m=1$, weil dann nicht acht, sondern nur vier verschiedene Darstellungen

$$(\pm 1, 0) \text{ und } (0, \pm 1)$$

existiren, die sich zu der einzigen Zerlegung $1 = 1^2 + 0^2$ vereinigen.

In diesem allgemeinen Resultat ist als specieller Fall der

berühmte von *Fermat* aufgestellte, zuerst von *Euler* *) bewiesene Satz enthalten:

Jede (positive) Primzahl von der Form $4h+1$ lässt sich stets, und zwar nur auf eine einzige Weise in zwei Quadrate zerfällen.

Die Bedingung, dass die Quadrate keinen gemeinschaftlichen Factor haben, fällt hier fort, da sie sich von selbst versteht.

Beispiel 1: Die Zahl 37 ist eine Primzahl von der Form $4h+1$; die beiden Wurzeln der Congruenz $z^2 \equiv -1 \pmod{37}$ findet man (z. B. mit Hülfe des Wilson'schen Satzes) $\equiv \pm 6$; nimmt man $n=6$, so hat man die Form $(37, 6, 1)$ zu betrachten, welche durch die Substitution $\binom{0,\ +1}{-1,\ -6}$ in die reducirte Form $(1, 0, 1)$ übergeht; umgekehrt geht also $(1, 0, 1)$ durch die inverse Substitution $\binom{-6,\ -1}{+1,\ 0}$ in $(37, 6, 1)$ über. Also ist die gesuchte Zerlegung folgende: $37 = 6^2 + 1^2$; es ist nicht nöthig, die vier zu dieser Wurzel $+6$, und die anderen vier zu der entgegengesetzten Wurzel -6 gehörenden Darstellungen hier einzeln aufzuschreiben.

Beispiel 2: Die Zahl $m = 65 = 5 \,.\, 13$ ist das Product aus den beiden Primzahlen 5 und 13, welche beide die Form $4h+1$ haben. Mithin giebt es $2^4 = 16$ verschiedene Darstellungen, also nur zwei verschiedene Zerlegungen der Zahl 65. Die vier Wurzeln der Congruenz $z^2 \equiv -1 \pmod{65}$ sind ± 8 und ± 18; wir bilden daher die beiden Formen $(65, 8, 1)$ und $(65, 18, 5)$, welche durch die Substitutionen $\binom{0,\ +1}{-1,\ -8}$ und $\binom{-1,\ -2}{+4,\ +7}$ in die reducirte Form $(1, 0, 1)$ übergehen; die inversen Substitutionen sind $\binom{-8,\ -1}{+1,\ 0}$ und $\binom{+7,\ +2}{-4,\ -1}$, und folglich sind die beiden gesuchten Zerlegungen folgende:

$$65 = 8^2 + 1^2 = 7^2 + 4^2.$$

§. 69.

Alle Formen der Determinante $D = -2$ bilden ebenfalls nur eine einzige Classe, da nur eine einzige reducirte Form

$$(1, 0, 2) = x^2 + 2y^2$$

vorhanden ist. Wir fragen auch hier wieder nach allen durch

*) *Demonstratio theorematis Fermatiani, omnem numerum primum formae $4n+1$ esse summam duorum quadratorum*, Nov. Comm. Petrop. V. p. 3.

diese Form darstellbaren *ungeraden* Zahlen m; die erste Bedingung ist die, dass -2 quadratischer Rest von m sein muss; dazu ist erforderlich und hinreichend, dass für jede in m aufgehende (also ungerade) Primzahl p

$$\left(\frac{-2}{p}\right) = +1,$$

also p von einer der beiden Formen $8h+1$ oder $8h+3$ sei. Umgekehrt: sind die sämmtlichen μ in m aufgehenden Primzahlen p alle von der Form $8h+1$ oder $8h+3$, so hat die Congruenz

$$z^2 \equiv -2 \pmod{m}$$

stets 2^μ incongruente Wurzeln. Ist n ein bestimmter Repräsentant einer solchen Wurzel, und $n^2+2 = ml$, so ist die Form (m, n, l) nothwendig der Form $(1, 0, 2)$ äquivalent; man findet daher (nach §. 66) eine Substitution $\binom{x,\ \xi}{y,\ \eta}$, durch welche die letztere in die erstere übergeht; ausser dieser existirt (nach §. 62) nur noch die andere $\binom{-x,\ -\xi}{-y,\ -\eta}$, welche dieselbe Eigenschaft hat; es giebt daher zwei verschiedene Darstellungen (x, y) und $(-x, -y)$ der Zahl m, die zu dieser Wurzel gehören. Im Ganzen giebt es daher

$$2 \cdot 2^\mu = 2^{\mu+1}$$

verschiedene Darstellungen der Zahl m durch die Form $(1, 0, 2)$.

Man erkennt ferner leicht, dass, wenn die beiden Darstellungen $\pm(x, y)$ zu der Wurzel n gehören, entsprechend die beiden Darstellungen $\pm(x, -y)$ zu der entgegengesetzten Wurzel $-n$ gehören. Je vier solche Darstellungen geben eine und dieselbe Zerlegung der Zahl m in ein Quadrat und ein doppeltes Quadrat; mithin ist die Anzahl aller verschiedenen Zerlegungen

$$= 2^{\mu-1};$$

die einzige Ausnahme bildet wieder der Fall, in welchem $\mu = 0$, also $m = 1$ ist; denn dann vereinigen sich die zwei verschiedenen Darstellungen ($+n$ ist $\equiv -n \pmod{1}$) zu der einzigen Zerlegung $1 = 1^2 + 2 \cdot 0^2$. Der interessanteste specielle Fall ist wieder der, in welchem $\mu = 1$ ist:

Jede Primzahl p von einer der beiden Formen $8h+1$ oder $8h+3$ lässt sich stets und nur auf eine einzige Weise in ein Quadrat und ein doppeltes Quadrat zerlegen.

Beispiel 1: Ist $m = 41$, so ist die Bedingung erfüllt; μ ist $= 1$; die beiden Wurzeln der Congruenz $z^2 \equiv -2 \pmod{41}$ sind ± 11; die Form $(41, 11, 3)$ geht durch die Substitution $\binom{-1,\ -1}{+4,\ +3}$ in

die Form (1, 0, 2) über, diese also rückwärts in jene durch die Substitution $\binom{+3,\ +1}{-4,\ -1}$; also ist $x = 3$, $y = -4$, und folglich

$$41 = 3^2 + 2 \cdot 4^2.$$

Beispiel 2: Ist $m = 33 = 3 \cdot 11$, so ist die Bedingung erfüllt; μ ist $= 2$, und folglich muss es zwei verschiedene Zerlegungen geben. Die Wurzeln der Congruenz $z^2 \equiv -2 \pmod{33}$ sind ± 8 und ± 14: wir bilden daher die beiden Formen (33, 8, 2) und (33, 14, 6), welche resp. durch die Substitutionen

$$\begin{pmatrix} -1, & 0 \\ +4, & -1 \end{pmatrix} \text{ und } \begin{pmatrix} -1, & +2 \\ +2, & -5 \end{pmatrix}$$

in die Form (1, 0, 2) übergehen; die inversen Substitutionen sind

$$\begin{pmatrix} -1, & 0 \\ -4, & -1 \end{pmatrix} \text{ und } \begin{pmatrix} -5, & -2 \\ -2, & -1 \end{pmatrix}$$

und folglich ist

$$33 = 1^2 + 2 \cdot 4^2 = 5^2 + 2 \cdot 2^2.$$

§. 70.

Alle Formen der Determinante $D = -3$ bilden *zwei* Classen, als deren Repräsentanten man die reducirten Formen

$$(1, 0, 3) = x^2 + 3y^2$$

und

$$(2, 1, 2) = 2x^2 + 2xy + 2y^2$$

annehmen kann; sie sind resp. von der ersten und zweiten Art. Ungerade Zahlen können offenbar nur durch die erstere dargestellt werden; es sei daher m eine ungerade und der Einfachheit wegen durch 3 nicht theilbare Zahl; damit sie durch die Form (1, 0, 3) darstellbar sei, ist erforderlich, dass, wenn p irgend eine in ihr aufgehende Primzahl ist,

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = +1,$$

folglich p von der Form $3h + 1$ sei. Umgekehrt, sobald diese Bedingung für alle μ in m aufgehenden Primzahlen p erfüllt ist, so hat die Congurenz

$$z^2 \equiv -3 \pmod{m}$$

stets 2^μ incongruente Wurzeln; ist n ein bestimmter Repräsentant

einer solchen, und $n^2 + 3 = ml$, so ist die Form (m, n, l) von der ersten Art (da m ungerade ist) und folglich der Form $(1, 0, 3)$ äquivalent. Es giebt also (nach §. 62) zwei Substitutionen

$$\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix} \text{ und } \begin{pmatrix} -x, & -\xi \\ -y, & -\eta \end{pmatrix}$$

durch welche die Form $(1, 0, 3)$ in die Form (m, n, l) übergeht, und folglich auch zwei Darstellungen (x, y) und $(-x, -y)$ der Zahl m, welche zu dieser Wurzel gehören. Im Ganzen giebt es daher

$$2 \cdot 2^\mu = 2^{\mu+1}$$

verschiedene Darstellungen einer solchen Zahl m durch die Form $(1, 0, 3)$, die sich aber wieder auf nur

$$\tfrac{1}{4} \cdot 2^{\mu+1} = 2^{\mu-1}$$

verschiedene Zerlegungen der Zahl m in ein einfaches und ein dreifaches Quadrat reduciren (nur auf den Fall $\mu = 0$, also $m = 1$ passt die letztere Formel wieder nicht). Besonders bemerkenswerth ist der specielle Fall:

Jede Primzahl von der Form $3h + 1$ ist stets und nur auf eine einzige Weise in ein einfaches und ein dreifaches Quadrat zerlegbar.

Gehen wir nun zu den durch die zweite Form $(2, 1, 2)$ darstellbaren, nothwendig geraden Zahlen über; wir beschränken uns auf diejenigen von der Form $2m$, wo m wieder eine ungerade und durch 3 nicht theilbare Zahl bedeutet. Dann erkennen wir leicht, dass der Complex dieser Zahlen m mit dem eben behandelten vollständig identisch ist. Denn aus der Möglichkeit der Congruenz $z^2 \equiv -3 \pmod{m}$ folgt auch die der Congruenz $z^2 \equiv -3 \pmod{2m}$, und umgekehrt (§. 37), und ausserdem ist die Anzahl der Wurzeln wieder $= 2^\mu$. Ist ferner n' ein bestimmter Repräsentant einer solchen, und $n'^2 + 3 = 2ml$, so ist die Form $(2m, n', l)$ nothwendig von der zweiten Art (denn der mittlere Coefficient n' ist ungerade, folglich l gerade) und also gewiss der Form $(2, 1, 2)$ äquivalent; man kann daher (nach §. 62) sechs verschiedene Transformationen der letztern Form in die erstere finden, aus welchen folgende sechs Darstellungen

$$\pm (x, y), \pm (y, -x - y), \pm (x + y, -x)$$

entspringen, die alle zu derselben Wurzel n' gehören (die sechs zu der entgegengesetzten Wurzel $-n'$ gehörenden Darstellungen

entstehen aus diesen durch Vertauschung der ersten darstellenden Zahl mit der zweiten)*). Im Ganzen existiren daher

$$6 \cdot 2^{\mu} = 3 \cdot 2^{\mu+1}$$

verschiedene Darstellungen der Zahl $2m$ durch die Form (2, 1, 2), oder, was dasselbe ist, der Zahl m durch die Form $x^2 + xy + y^2$. Sieht man je vier zusammengehörige Darstellungen von der Form

$$(x, y), \quad (-x, -y), \quad (y, x), \quad (-y, -x)$$

als nicht wesentlich verschieden an, so ist die Anzahl der wesentlich verschiedenen Darstellungen nur noch

$$= 3 \cdot 2^{\mu-1}.$$

Für eine Primzahl p von der Form $3h + 1$ giebt es daher immer drei wesentlich verschiedene Darstellungen durch die Form $x^2 + xy + y^2$.

Beispiel: Ist $m = 13$, so sind $n = \pm 7$ die Wurzeln der Congruenz $z^2 \equiv -3$ (mod. 26) und also auch der Congruenz $z^2 \equiv -3$ (mod. 13). Wir bilden daher die beiden Formen (13, 7, 4) und (26, 7, 2). Sie gehen resp. durch die Substitutionen

$$\begin{pmatrix} -1, & -1 \\ +2, & +1 \end{pmatrix} \text{ und } \begin{pmatrix} 0, & +1 \\ -1, & -4 \end{pmatrix}$$

in die Formen (1, 0, 3) und (2, 1, 2) über. Die beiden inversen Substitutionen sind

$$\begin{pmatrix} +1, & +1 \\ -2, & -1 \end{pmatrix} \text{ und } \begin{pmatrix} -4, & -1 \\ +1, & 0 \end{pmatrix}$$

und folglich ist

$$13 = 1^2 + 3\,(-2)^2 = (-4)^2 + (-4) \cdot 1 + 1^2;$$

hieraus findet man leicht die beiden anderen Darstellungen

$$13 = 4^2 + 4 \cdot (-3) + (-3)^2$$
$$= 3^2 + 3 \cdot 1 + 1^2$$

*) Da von den Zahlen x, y, $x + y$ stets eine und nur eine gerade ist, so giebt es unter den sechs zu der Wurzel n' gehörenden Darstellungen der Zahl $2m$ immer zwei $\pm (x', y')$, in welchen y' gerade ist $= 2u$; setzt man ferner $x' + u = t$, so geht die Gleichung $x'x' + x'y' + y'y' = m$ über in $tt + 3uu = m$, d. h. man erhält eine Darstellung (t, u) der Zahl m durch die Form (1, 0, 3), und zwar gehört diese Darstellung zu derselben Wurzel n'. Hierin besteht der Zusammenhang zwischen den Darstellungen der Zahlen m und $2m$ resp. durch die Formen (1, 0, 3) und (2, 1, 2).

§. 71.

Als letztes Beispiel wählen wir die Determinante $D = -5$; es giebt *zwei* nicht äquivalente reducirte Formen

$$(1, 0, 5) \text{ und } (2, 1, 3),$$

beide sind ursprünglich und von der ersten Art. Wir suchen wieder das System aller ungeraden und durch 5 nicht theilbaren Zahlen m zu bestimmen, welche durch diese Formen darstellbar sind. Die dazu erforderliche Bedingung besteht darin, dass für jede in m aufgehende Primzahl p die Gleichung

$$\left(\frac{-5}{p}\right) = (-1)^{\frac{1}{2}(p-1)}\left(\frac{p}{5}\right) = +1$$

Statt finden muss; hieraus folgt (§. 52, II), dass jede solche Primzahl von einer der vier Formen

$$20h+1,\quad 20h+9,\quad 20h+3,\quad 20h+7$$

sein muss. Ist diese Bedingung erfüllt, und μ die Anzahl der verschiedenen Primzahlen p, so hat die Congruenz

$$z^2 \equiv -5 \pmod{m}$$

wieder 2^μ incongruente Wurzeln; ist n ein bestimmter Repräsentant einer solchen, und $n^2 + 5 = ml$, so ist die Form (m, n, l) nothwendig einer und nur einer der beiden obigen reducirten Formen äquivalent; es giebt dann jedesmal (nach §. 62) zwei Substitutionen, durch welche diese reducirte Form in (m, n, l) übergeht, also auch zwei zu der Wurzel n gehörige Darstellungen der Zahl m durch diese reducirte Form. Im Ganzen giebt es also

$$2 \cdot 2^\mu = 2^{\mu+1}$$

Darstellungen einer solchen Zahl durch die obigen reducirten Formen. Allein es bleibt noch zweifelhaft, durch welche der beiden reducirten Formen die zu einer bestimmten Wurzel n gehörigen beiden Darstellungen erfolgen; und eine ähnliche Frage wird jedesmal da auftreten, wo es mehrere nicht äquivalente Formen derselben Art giebt. In unserm Fall ist es nicht schwierig, diesen Zweifel zu heben.

Ist nämlich die Zahl m darstellbar durch die Form $(1, 0, 5)$, also z. B. $m = x^2 + 5y^2$, so folgt hieraus $m \equiv x^2 \pmod{5}$, d. h.

m ist quadratischer Rest von 5; ist dagegen die Zahl m darstellbar durch die zweite Form (2, 1, 3), also z. B. $m = 2x^2 + 2xy + 3y^2$, so ist $2m = (2x + y)^2 + 5y^2 \equiv (2x + y)^2 \pmod{5}$, und, da 2 quadratischer Nichtrest von 5 ist, so ist m ebenfalls quadratischer Nichtrest von 5. Es tritt also hier die besonders einfache Erscheinung auf, dass alle Darstellungen einer Zahl entweder nur durch die Form (1, 0, 5) oder nur durch die Form (2, 1, 3) geschehen, je nachdem m quadratischer Rest oder Nichtrest von 5, d. h. je nachdem $m \equiv \pm 1$, oder $\equiv \pm 2 \pmod{5}$ ist. Hieraus folgen die speciellen Sätze:

Jede Primzahl von einer der beiden Formen $20h + 1$, $20h + 9$ ist auf vier Arten durch die Form (1, 0, 5) darstellbar (welche wesentlich nur eine einzige Zerlegung in ein einfaches und ein fünffaches Quadrat bilden); jede Primzahl von einer der beiden Formen $20h + 3$, $20h + 7$ ist auf vier Arten durch die Form (2, 1, 3) darstellbar.

Beispiel 1: Ist $m = 29$, so sind $n = \pm 13$ die beiden Wurzeln der Congruenz $z^2 \equiv -5 \pmod{29}$; die hieraus gebildete Form (29, 13, 6) geht durch die Substitution

$$\begin{pmatrix} -1, & +1 \\ +2, & -3 \end{pmatrix}$$

in die reducirte Form (1, 0, 5) über; durch Umkehrung dieser Substitution erhält man die Zerlegung

$$29 = 3^2 + 5 \cdot 2^2.$$

Beispiel 2: Für $m = 27$ findet man $n = \pm 7$; die beiden entsprechenden Formen (27, 7, 2) und (27, -7, 2) gehen bezüglich durch die Substitutionen

$$\begin{pmatrix} 0, & +1 \\ -1, & -4 \end{pmatrix} \text{ und } \begin{pmatrix} 0, & 1 \\ -1, & 3 \end{pmatrix}$$

in die reducirte Form (2, 1, 3) über; durch Umkehrung derselben erhält man daher die vier Darstellungen

$$27 = 2(\mp 4)^2 + 2(\mp 4)(\pm 1) + 3(\pm 1)^2$$
$$27 = 2(\pm 3)^2 + 2(\pm 3)(\pm 1) + 3(\pm 1)^2$$

von denen die beiden ersteren zu der Wurzel $+7$, die beiden letzteren zu der Wurzel -7 gehören.

§. 72.

Wir wenden uns nun zu den Formen mit *positiver* Determinante D, um auch für sie die Hauptprobleme der Theorie der Aequivalenz zu lösen. Das zweite Problem (§. 59), aus *einer* Transformation einer Form in eine zweite *alle* Transformationen der erstern in die letztere zu finden, ist durch unsere frühere Untersuchung (§. 62) auf die Aufgabe zurückgeführt, alle ganzzahligen Auflösungen der Gleichung

$$t^2 - Du^2 = \sigma^2$$

zu finden. Dieselbe ist für positive Determinanten bei weitem schwieriger zu lösen, als für negative. Dasselbe gilt von dem ersten Hauptproblem: zu erkennen, ob zwei Formen von gleicher Determinante äquivalent sind oder nicht. Wir schlagen zur Lösung desselben einen ganz andern Weg ein, wie früher bei negativen Determinanten, einen Weg, der aber zugleich die Mittel an die Hand geben wird, auch die obige Gleichung vollständig aufzulösen.*)

Das Charakteristische dieser Methode besteht darin, dass wir auch *irrationale* Grössen in den Kreis unserer Betrachtungen ziehen. Ist nämlich (a, b, c) oder

$$ax^2 + 2bxy + cy^2$$

eine Form, deren Determinante $b^2 - ac = D$ positiv ist, so hat die entsprechende quadratische Gleichung

$$a + 2b\omega + c\omega^2 = 0$$

zwei reelle Wurzeln

$$\omega = \frac{-b \mp \sqrt{D}}{c} = \frac{a}{-b \pm \sqrt{D}},$$

die wir, je nachdem das obere oder untere Zeichen genommen wird, als die *erste* oder *zweite Wurzel der Form* (a, b, c) bezeichnen und von einander unterscheiden wollen, indem wir ein für alle Mal festsetzen, dass das Zeichen $\sqrt{D}$ stets die *positive* Quadratwurzel aus der Determinante bedeuten soll. Durch die Coefficienten der Form (a, b, c) ist also jede ihrer beiden Wurzeln vollständig, ohne Zweideutigkeit bestimmt. Aber umgekehrt ist auch jede Form (a, b, c) der Determinante D durch Angabe *einer* ihrer

*) *Lejeune Dirichlet: Vereinfachung der Theorie der binären quadratischen Formen von positiver Determinante* (Berliner Akad. 1854).

Wurzeln vollständig charakterisirt, in der Weise, dass zwei Formen (a, b, c) und (a', b', c') *derselben* Determinante D nothwendig identisch sind, sobald sie gleiche erste, oder gleiche zweite Wurzeln haben; denn aus der Gleichung

$$\frac{-b' \mp \sqrt{D}}{c'} = \frac{-b \mp \sqrt{D}}{c},$$

worin entweder die beiden oberen, oder die beiden unteren Zeichen zu nehmen sind, ergiebt sich in Folge der Irrationalität von $\sqrt{D}$ zunächst $c' = c$, und dann $b' = b$, also auch $a' = a$.

Im Folgenden nennen wir zwei Wurzeln ω, ω' zweier Formen resp. (a, b, c), (a', b', c') *gleichnamig*, wenn beide erste, oder beide zweite Wurzeln sind, *ungleichnamig* dagegen, wenn die eine die erste, die andere die zweite Wurzel ist. Wir können dann das eben erhaltene Resultat auch so aussprechen: *Wenn zwei Formen dieselbe (positive) Determinante besitzen, und wenn eine Wurzel der einen Form mit der gleichnamigen Wurzel der andern Form übereinstimmt, so sind beide Formen identisch.*

§. 73.

Wir wollen nun annehmen, es seien (a, b, c) und (a', b', c') zwei äquivalente Formen, und zwar wollen wir für einen Augenblick die uneigentliche Aequivalenz nicht ausschliessen, weil dadurch der Nerv der Betrachtung deutlicher hervortritt. Es sei $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ eine Substitution, durch welche (a, b, c) in (a', b', c') übergeht, also

$$\alpha\delta - \beta\gamma = \varepsilon = \pm 1.$$

Da durch diese Substitution

$$x = \alpha x' + \beta y',\ y = \gamma x' + \delta y'$$

identisch

$$ax^2 + 2bxy + cy^2 = a'x'^2 + 2b'x'y' + c'y'^2$$

wird, so leuchtet ein, dass vermöge der Formeln

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'},\quad \omega' = \frac{-\gamma + \alpha\omega}{\delta - \beta\omega}$$

aus einer Wurzel ω' der Form (a', b', c') eine Wurzel ω der Form (a, b, c) gefunden werden kann, und umgekehrt; denn die Wurzeln

dieser Formen sind ja die Werthe der Verhältnisse $y:x$ und $y':x'$, für welche die Formen verschwinden. Aber es fragt sich vor allen Dingen, ob zwei so verbundene Wurzeln ω und ω' gleichnamig sind, oder nicht. Da nun

$$\omega = \frac{-b \mp \sqrt{D}}{c}$$

ist, so folgt

$$\omega' = \frac{\gamma c - \alpha(-b \mp \sqrt{D})}{-\delta c + \beta(-b \mp \sqrt{D})} = \frac{b\alpha + c\gamma \pm \alpha\sqrt{D}}{-b\beta - c\delta \mp \beta\sqrt{D}};$$

machen wir den Nenner rational, indem wir den Bruch durch $-b\beta - c\delta \pm \beta\sqrt{D}$ erweitern und berücksichtigen, dass

$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b'$$

$$a\beta^2 + 2b\beta\delta + c\delta^2 = c'$$

ist, so ergiebt sich

$$\omega' = \frac{-b' \mp \varepsilon\sqrt{D}}{c'}.$$

Wir haben daher folgendes Resultat erhalten: *Wenn eine Form (a, b, c) durch eine Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ in eine äquivalente Form (a', b', c') übergeht, so ist je eine Wurzel ω der erstern mit je einer Wurzel ω' der letztern Form durch die Relation*

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'},\quad \omega' = \frac{-\gamma + \alpha\omega}{\delta - \beta\omega}$$

verbunden; und zwar bilden ω, ω' ein Paar gleichnamiger oder ungleichnamiger Wurzeln der beiden Formen, je nachdem die Substitution eine eigentliche oder uneigentliche ist.

Wir schliessen von jetzt an uneigentliche Aequivalenz und uneigentliche Substitutionen gänzlich aus; es sind dann also stets zwei *gleichnamige* Wurzeln der beiden äquivalenten Formen in der angegebenen Weise mit einander verbunden. Dieser Satz lässt sich in folgender Weise umkehren:

Wenn zwei Formen (a, b, c), (a', b', c') dieselbe Determinante haben, und wenn zwei gleichnamige Wurzeln ω und ω' derselben durch die Gleichung

$$\omega = \frac{\gamma + \delta\omega'}{\alpha + \beta\omega'}$$

verbunden sind, in welcher die vier ganzen Zahlen α, β, γ, δ der Gleichung

$$\alpha\delta - \beta\gamma = 1$$

genügen, so sind die beiden Formen äquivalent, und zwar geht die erstere durch die Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ *in die letztere über.*

Denn durch diese Substitution geht (a, b, c) in eine äquivalente Form (a'', b'', c'') über, und bezeichnet man mit ω'' ihre mit ω gleichnamige Wurzel, so ist nach dem eben bewiesenen Satze

$$\omega = \frac{\gamma + \delta\omega''}{\alpha + \beta\omega''}, \text{ und folglich } \omega' = \omega'';$$

da ferner der Voraussetzung nach ω' mit ω, folglich auch mit ω'' gleichnamig ist, und da endlich (a', b', c') dieselbe Determinante wie (a, b, c), und folglich auch wie (a'', b'', c'') hat, so ist zufolge der Schlussbemerkung des vorigen Paragraphen (a', b', c') identisch mit (a'', b'', c''), d. h. (a, b, c) geht durch die obige Substitution in (a', b', c') über.

Von besonderer Wichtigkeit für das Folgende ist die Betrachtung zweier *benachbarten* Formen (a, b, a') und (a', b', a''), in welchen der Definition zufolge (§. 63) die Summe $b + b'$ durch a' theilbar, also $b + b' = -a'\delta$ ist, und von welchen die erstere in die letztere durch die Substitution $\binom{0,\ 1}{-1,\ \delta}$ übergeht. Die gleichnamigen Wurzeln ω und ω' dieser beiden Formen hängen durch die Gleichungen

$$\omega = \delta - \frac{1}{\omega'},\ \omega' = \frac{1}{\delta - \omega}$$

zusammen.

§. 74.

Auch bei positiven Determinanten vergleicht man zwei Formen, deren Aequivalenz beurtheilt werden soll, nicht unmittelbar mit einander, sondern man transformirt jede von ihnen in eine sogenannte *reducirte**) Form; der Begriff einer solchen ist aber hier wesentlich verschieden von demjenigen, welcher früher (§. 64) für negative Determinanten aufgestellt ist.

Eine Form (a, b, c) von positiver Determinante D heisst eine reducirte Form, wenn, abgesehen vom Zeichen, ihre erste Wurzel

---

*) *Gauss: D. A.* art. 1 3.

$$\frac{-b-\sqrt{D}}{c} > 1,$$

ihre zweite Wurzel

$$\frac{-b+\sqrt{D}}{c} < 1$$

ist, und wenn ausserdem beide Wurzeln entgegengesetzte Zeichen haben.

Ziehen wir zunächst einige Folgerungen aus dieser Erklärung. Da die erste Wurzel numerisch grösser als die zweite, also auch die Summe der beiden Grössen b und $\sqrt{D}$ numerisch grösser als ihre Differenz sein soll, so muss, da $\sqrt{D}$ positiv ist, auch b positiv sein (nicht $= 0$); da ferner die beiden Wurzeln entgegengesetzte Zeichen haben, so gilt dasselbe auch von den beiden Grössen

$$-(b+\sqrt{D}) \quad \text{und} \quad -b+\sqrt{D};$$

und da die erstere gewiss negativ ist, so muss die letztere positiv sein; es ist daher

$$0 < b < \sqrt{D}.$$

Bezeichnen wir ferner mit (c) wieder den absoluten Werth des Coefficienten c, so muss also im algebraischen Sinne (d. h. mit Rücksicht auf die Vorzeichen)

$$\frac{b+\sqrt{D}}{(c)} > 1 \quad \text{und} \quad 0 < \frac{-b+\sqrt{D}}{(c)} < 1,$$

d. h. es muss

$$0 < \sqrt{D}-b < (c) < \sqrt{D}+b$$

sein; und umgekehrt leuchtet ein, dass jede Form (a, b, c), deren Coefficienten diesen letzteren Ungleichungen genügen, sicher eine reducirte Form ist, weil aus ihnen rückwärts die ursprünglichen Bedingungen sich ableiten lassen.

Aus der Definition ergeben sich noch weitere Folgerungen. Da $D = b^2 - ac$ und $b^2 < D$ ist, so müssen a und c entgegengesetzte Zeichen haben; da ferner die erste Wurzel und c ebenfalls entgegengesetzte Zeichen haben, so hat die erste Wurzel dasselbe Vorzeichen wie der erste Coefficient a der Form. Nun hat ferner die zweite Wurzel das entgegengesetzte Zeichen der ersten Wurzel, also dasselbe Vorzeichen wie der dritte Coefficient c der Form, was sich unmittelbar auch daraus ergiebt, dass $\sqrt{D}-b$ positiv ist.

Für den absoluten Werth des ersten Coefficienten a gelten dieselben Bedingungen, wie für den von c; denn da

$$D = b^2 + (a)(c),$$

also

$$(a) = \frac{(\sqrt{D} + b)(\sqrt{D} - b)}{(c)}$$

ist, so ergiebt sich aus den Bedingungen

$$\frac{\sqrt{D} + b}{(c)} > 1, \quad 0 < \frac{\sqrt{D} - b}{(c)} < 1,$$

dass

$$(a) > \sqrt{D} - b, \quad \text{und} \quad (a) < \sqrt{D} + b$$

ist *).

Für das Folgende ist noch der specielle Fall bemerkenswerth, in welchem

$$\sqrt{D} - (a) < b < \sqrt{D} \text{ und } (c) \geqq (a)$$

ist; aus diesen Bedingungen kann man nämlich stets schliessen, dass die Form (a, b, c) reducirt ist, obwohl die Umkehrung nicht gestattet ist. In der That, giebt man diesen Bedingungen die Form

$$0 < \sqrt{D} - b < (a) \lesseqgtr (c),$$

so ergiebt sich zunächst, dass die zweite Wurzel

$$\frac{-b + \sqrt{D}}{c}$$

numerisch < 1, ferner dass die erste Wurzel

$$\frac{-b - \sqrt{D}}{c} = \frac{a}{\sqrt{D} - b}$$

numerisch > 1 ist. Hieraus folgt weiter, wie oben, dass b positiv ist, weil $\sqrt{D} + b$ numerisch grösser als $\sqrt{D} - b$ ist; und folglich haben, da ausserdem $b < \sqrt{D}$ ist, beide Wurzeln entgegengesetzte Zeichen. Also ist die Form gewiss eine reducirte.

*) Dasselbe ergiebt sich unmittelbar daraus, dass die erste Wurzel einer Form (a, b, c) der reciproke Werth der zweiten Wurzel ihres *Gefährten* (c, b, a) ist; mithin sind entweder beide Formen reducirt, oder beide nicht reducirt.

§. 75.

Aus der Erklärung einer reducirten Form ergiebt sich ferner der folgende wichtige Satz*) (vergl. §. 67):

Für jede positive Determinante giebt es nur eine endliche Anzahl reducirter Formen.

Denn, bezeichnen wir mit λ die grösste ganze in $\sqrt{D}$ enthaltene Zahl, so dass $\lambda < \sqrt{D} < \lambda + 1$ und also λ mindestens $= 1$ ist, so kann der mittlere Coefficient b einer reducirten Form (a, b, c) nur die λ verschiedenen Werthe $1, 2 \ldots \lambda$ haben; für jeden dieser Werthe von b ist $D - b^2 = (a)(c)$ auf alle mögliche Arten in zwei Factoren zu zerlegen, welche zwischen $\lambda - b$ und $\lambda + 1 + b$ exclusive (oder zwischen $\lambda + 1 - b$ und $\lambda + b$ inclusive) liegen; je zwei solchen Factoren a und c hat man entgegengesetzte Zeichen zu geben, und man muss sie permutiren, wenn sie ungleich sind. Dann sind aber wirklich alle reducirten Formen gefunden, und es giebt deren offenbar nur eine endliche Anzahl.

Beispiel 1: Ist $D = 13$, so ist $\lambda = 3$; wir haben daher folgende Fälle und Zerlegungen:

$$b = 1;\quad 12 = 3 \,.\, 4$$
$$b = 2;\quad 9 = 3 \,.\, 3$$
$$b = 3;\quad 4 = 1 \,.\, 4 = 2 \,.\, 2$$

und diese liefern die folgenden 12 reducirten Formen:

$$(\pm 3, 1, \mp 4), (\pm 1, 3, \mp 4), (\pm 3, 2, \mp 3),$$
$$(\pm 4, 1, \mp 3), (\pm 4, 3, \mp 1), (\pm 2, 3, \mp 2).$$

Beispiel 2: Für $D = 19$ ist $\lambda = 4$; wir bilden daher folgende Tabelle:

$$b = 1;\quad 18 \text{ giebt keine Zerlegung};$$
$$b = 2;\quad 15 = 3 \,.\, 5;$$
$$b = 3;\quad 10 = 2 \,.\, 5;$$
$$b = 4;\quad 3 = 1 \,.\, 3;$$

hieraus ergeben sich folgende 12 reducirte Formen:

$$(\pm 3, 2, \mp 5), (\pm 2, 3, \mp 5), (\pm 1, 4, \mp 3),$$
$$(\pm 5, 2, \mp 3), (\pm 5, 3, \mp 2), (\pm 3, 4, \mp 1).$$

*) *Gauss: D. A.* art. 185.

Beispiel 3: Für $D = 35$ ist $\lambda = 5$; also bilden wir die Tabelle

$b = 1$; 34 giebt keine Zerlegung;
$b = 2$; 31 " " "
$b = 3$; 26 " " "
$b = 4$; 19 " " "
$b = 5$; $10 = 1 \,.\, 10 = 2 \,.\, 5$;

wir erhalten daher 8 reducirte Formen:

$(\pm 1, 5, \mp 10)$, $(\pm 2, 5, \mp 5)$;
$(\pm 10, 5, \mp 1)$, $(\pm 5, 5, \mp 2)$.

Beispiel 4: Für $D = 79$ ist $\lambda = 8$; wir bilden daher folgende Tabelle:

$b = 1$; 78 giebt keine Zerlegung;
$b = 2$; 75 " " "
$b = 3$; $70 = 7 \,.\, 10$;
$b = 4$; $63 = 7 \,.\, 9$;
$b = 5$; $54 = 6 \,.\, 9$;
$b = 6$; 43 giebt keine Zerlegung;
$b = 7$; $30 = 2 \,.\, 15 = 3 \,.\, 10 = 5 \,.\, 6$;
$b = 8$; $15 = 1 \,.\, 15 = 3 \,.\, 5$;

wir erhalten daher 32 reducirte Formen:

$(\pm 7, 3, \mp 10)$, $(\pm 7, 4, \mp 9)$, $(\pm 6, 5, \mp 9)$, $(\pm 2, 7, \mp 15)$,
$(\pm 3, 7, \mp 10)$, $(\pm 5, 7, \mp 6)$, $(\pm 1, 8, \mp 15)$, $(\pm 3, 8, \mp 5)$,

und

$(\pm 10, 3, \mp 7)$, $(\pm 9, 4, \mp 7)$, $(\pm 9, 5, \mp 6)$, $(\pm 15, 7, \mp 2)$,
$(\pm 10, 7, \mp 3)$, $(\pm 6, 7, \mp 5)$, $(\pm 15, 8, \mp 1)$, $(\pm 5, 8, \mp 3)$.

§. 76.

Aehnlich wie bei negativen Determinanten (§. 64) beweisen wir auch die Richtigkeit des folgenden Satzes*):

Jede Form von positiver Determinante ist einer reducirten Form äquivalent.

Bezeichnen wir die gegebene Form von positiver Determinante

*) *Gauss: D. A.* art. 183.

D mit (a, b, a'), so suchen wir eine ihr nach rechts benachbarte Form (a', b', a'') so zu bestimmen, dass

$$\sqrt{D} - (a') < b' < \sqrt{D}$$

wird. Da zufolge der Erklärung einer benachbarten Form der mittlere Coefficient b' jeden Werth erhalten kann, welcher $\equiv -b$ (mod. a') ist, und keinen andern, so fragt sich nur, ob zwischen den Grenzen $\sqrt{D} - (a')$ und $\sqrt{D}$ stets ein solcher Werth existirt; dies ist offenbar der Fall, da die sämmtlichen zwischen diesen beiden Grenzen enthaltenen ganzen Zahlen

$$\lambda + 1 - (a'), \quad \lambda + 2 - (a') \ldots \lambda - 1, \quad \lambda$$

ein vollständiges Restsystem in Bezug auf den Modulus a' bilden; aus demselben Grunde ergiebt sich, dass nur eine einzige solche Zahl b' existirt. Nachdem $b' = -b - a'\delta$ bestimmt ist, geht die Form (a, b, a') durch die Substitution $\binom{0,\ 1}{-1,\ \delta}$ in die benachbarte Form (a', b', a'') über, deren Coefficienten a', b' der obigen Bedingung Genüge leisten. Findet sich nun, dass zu gleicher Zeit $(a'') \geqq (a')$ wird, so ist nach dem am Schlusse des §. 74 besonders hervorgehobenen speciellen Fall die gefundene Form (a', b', a'') eine reducirte. Ist dagegen

$$(a') > (a''),$$

so verfahre man mit der gefundenen Form (a', b', a'') genau so wie mit der gegebenen Form, d. h. man bilde die ihr nach rechts benachbarte Form (a'', b'', a'''), in welcher

$$\sqrt{D} - (a'') < b'' < \sqrt{D}$$

ist, und welche gewiss eine reducirte ist, wenn $(a''') \geqq (a'')$ ist. Sollte aber wieder

$$(a'') > (a''')$$

sein, so setze man denselben Process in derselben Weise fort; da unter einer gegebenen positiven Zahl (a') nur eine endliche Anzahl von ganzen positiven Zahlen liegt, so muss man nach einer endlichen Anzahl von Transformationen durchaus zu einer Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$, in welcher sowohl

$$\sqrt{D} - (a^{(n)}) < b^{(n)} < \sqrt{D}$$

als auch

$$(a^{(n+1)}) \geqq (a^{(n)})$$

ist, also zu einer reducirten Form gelangen, was zu beweisen war.

Es verdient bemerkt zu werden, dass bei diesem Process nicht gerade erst die letzte Form eine reducirte zu sein braucht, denn

es giebt reducirte Formen, in welchen die Bedingungen des besondern hier benutzten speciellen Falles nicht erfüllt sind. Von grösserer Wichtigkeit ist es aber, besonders darauf aufmerksam zu machen, dass durch den angegebenen Process auch jedes Mal eine Substitution gefunden wird, durch welche die gegebene Form in die reducirte Form übergeht, und zwar erhält man diese Substitution durch Composition der successiven Substitutionen, welche in dem Processe auftreten. Der Algorithmus selbst ist durchaus nicht beschwerlich (vergl. §. 64), wie folgende Beispiele zeigen.

Beispiel 1: Die Form (4, 6, 7) hat die Determinante $D = 8$; es ist also $\lambda = 2$. Unter den Zahlen

$$-4, \; -3, \; -2, \; -1, \; 0, \; 1, \; 2$$

ist $b' = 1 \equiv -6 \pmod{7}$; dies giebt die benachbarte Form $(7, 1, -1)$, welche noch nicht reducirt ist. Da $(a'') = 1$ ist, so ist $b'' = \lambda = 2$, und folglich erhält man die benachbarte Form $(-1, 2, 4)$, welche wirklich reducirt ist. Durch die Substitution $\begin{pmatrix} 0, & +1 \\ -1, & -1 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 3 \end{pmatrix} = \begin{pmatrix} -1, & +3 \\ +1, & -4 \end{pmatrix}$ geht die gegebene Form in die gefundene über.

Beispiel 2: Die Form (713, 60, 5) hat die Determinante $D = 35$; man findet nach der angegebenen Methode die nach rechts benachbarte Form $(5, 5, -2)$, und zu dieser wieder die Form $(-2, 5, 5)$, in welcher der letzte Coefficient in der That grösser ist als der erste. In diesem Beispiel ist aber auch schon die vorhergehende Form $(5, 5, -2)$ reducirt. Die gegebene Form geht durch die Substitution $\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix}$ in $(5, 5, -2)$ und durch die Substitutiou $\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix} = \begin{pmatrix} -1, & +5 \\ 13, & -66 \end{pmatrix}$ in $(-2, 5, 5)$ über.

Beispiel 3: Die Form (62, 95, 145), deren Determinante $D = 35$, geht durch die folgenden successiven Substitutionen

$$\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \; \begin{pmatrix} 0, & 1 \\ -1, & 2 \end{pmatrix}, \; \begin{pmatrix} 0, & 1 \\ -1, & 2 \end{pmatrix}, \; \begin{pmatrix} 0, & 1 \\ -1, & 4 \end{pmatrix}$$

successive in die Formen

$$(145, -95, 62), \quad (62, -29, 13), \quad (13, 3, -2), \quad (-2, 5, 5)$$

über, von denen erst die letzte reducirt ist; die Zusammensetzung dieser Substitutionen giebt die Substitution $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$, durch welche (62, 95, 145) in $(-2, 5, 5)$ übergeht.

§. 77.

Nachdem in den beiden vorhergehenden Paragraphen dargethan ist, dass jede Form von positiver Determinante einer reducirten Form äquivalent ist, und dass nur eine endliche Anzahl von reducirten Formen für jede gegebene Determinante existirt, so folgt hieraus unmittelbar:

Die Anzahl der Classen nicht äquivalenter Formen von positiver Determinante ist stets endlich.

Allein es bleibt noch die Hauptfrage zu beantworten, ob zwei nicht identische reducirte Formen derselben Determinante einander äquivalent sein können; denn erst dann haben wir (wie in §§. 65, 66 für negative Determinanten) die Mittel gewonnen, um über die Aequivalenz von zwei gegebenen Formen derselben positiven Determinante entscheiden zu können. Diese Untersuchung stösst bei positiven Determinanten auf bedeutende Schwierigkeiten, da in der That immer mehrere nicht identische und doch äquivalente reducirte Formen existiren.

Um einen sichern Boden für diese Untersuchung zu gewinnen, stellen wir zunächst die bestimmte Frage *):

Kann eine reducirte Form (a, b, a') eine ihr nach rechts benachbarte Form (a', b', a'') haben, welche ebenfalls reducirt ist?

Nehmen wir einmal an, dies sei möglich, und es sei $\binom{0,\ 1}{-1,\ \delta}$ die Substitution, durch welche die reducirte Form (a, b, a') in die ebenfalls reducirte Form (a', b', a'') übergeht. Sind dann ω und ω' zwei gleichnamige Wurzeln der ersten und der zweiten Form, so hängen diese (nach §. 73) durch die Gleichungen

$$\omega = \delta - \frac{1}{\omega'},\quad \omega' = \frac{1}{\delta - \omega}$$

mit einander zusammen. Wir wollen der Einfachheit halber festsetzen, dass ω und ω' die beiden *ersten* Wurzeln der beiden Formen bedeuten (obgleich dieselbe Relation auch zwischen den beiden zweiten Wurzeln Statt findet). Da in einer reducirten Form die beiden äusseren Coefficienten entgegengesetzte Zeichen haben, und die erste Wurzel stets das Zeichen des ersten Coefficienten besitzt, so haben die beiden *unechten* Brüche ω und ω' bezüglich die Vorzeichen von a und a', also *entgegengesetzte* Vorzeichen, da der erste

*) *Gauss: D. A.* art. 184.

Coefficient a' der zweiten Form zugleich der letzte Coefficient der ersten Form ist. Zufolge der obigen Relationen muss daher $\omega - \delta$ ein *echter* Bruch sein von gleichem Vorzeichen wie ω; es muss daher δ diejenige vollständig bestimmte ganze Zahl sein, welche dem absoluten Werth nach nächst kleiner als ω ist und dem Vorzeichen nach mit ω übereinstimmt. Wir schliessen hieraus, dass eine reducirte Form (a, b, a') höchstens eine einzige nach rechts benachbarte Form (a', b', a'') hat, welche ebenfalls reducirt ist.

Aber es existirt auch wirklich immer eine solche der reducirten Form (a, b, a') nach rechts benachbarte und reducirte Form (a', b', a''). Denn es sei ω die erste Wurzel der reducirten Form (a, b, a'), also ein unechter Bruch, dessen Vorzeichen mit dem von a übereinstimmt; so wähle man die ganze Zahl δ so, dass ihr absoluter Werth (δ) die grösste ganze in (ω) enthaltene ganze Zahl (also nie $= 0$) wird, und gebe δ das Vorzeichen von ω; dann geht die gegebene Form (a, b, a') durch die so bestimmte Substitution $\left(\begin{smallmatrix} 0, & 1 \\ -1, & \delta \end{smallmatrix}\right)$ in eine benachbarte Form (a', b', a'') über, deren erste Wurzel

$$\omega' = \frac{1}{\delta - \omega}$$

ein unechter Bruch ist, dessen Vorzeichen dem von ω und a entgegengesetzt ist und also mit dem von a' übereinstimmt. Bezeichnen wir nun mit ω_1 und ω'_1 die beiden zweiten Wurzeln, so besteht zwischen ihnen dieselbe Relation

$$\omega'_1 = \frac{1}{\delta - \omega_1};$$

da nun ω_1 ein echter Bruch ist, dessen Vorzeichen dem von ω, und also auch dem von δ entgegengesetzt, und da δ eine von Null verschiedene ganze Zahl ist, so folgt, dass $\delta - \omega_1$ ein unechter Bruch, und also ω'_1 ein echter Bruch ist, dessen Vorzeichen mit dem von δ, ω und a übereinstimmt, also dem von ω' und a' entgegengesetzt ist. Es ist also bewiesen, dass die beiden Wurzeln ω' und ω'_1 der neuen Form (a', b', a'') entgegengesetzte Zeichen haben, ferner dass die erste ω' ein unechter, die zweite ω'_1 ein echter Bruch ist; folglich ist diese Form in der That eine reducirte, was zu beweisen war.

Jede reducirte Form hat daher eine und nur eine nach rechts benachbarte Form, welche ebenfalls reducirt ist, und diese kann auf die angegebene Weise immer leicht gefunden werden.

Genau ebenso liesse sich nun auch beweisen, dass jede redu-

cirte Form eine und nur eine nach links benachbarte reducirte Form besitzt. Doch ist es bequemer, diesen Fall auf den eben behandelten durch die einleuchtende Bemerkung (§. 74 Anm.) zurückzuführen, dass die beiden Formen (a, b, a') und (a', b, a) gleichzeitig reducirte, oder gleichzeitig nicht reducirte Formen sind. Wenn nun die reducirte Form (a, b, a') eine nach links benachbarte und ebenfalls reducirte Form $('a, 'b, a)$ besitzt, so hat die reducirte Form (a', b, a) die nach rechts benachbarte Form $(a, 'b, 'a)$, welche ebenfalls reducirt ist; und umgekehrt, sobald die Form $(a, 'b, 'a)$ der reducirten Form (a', b, a) nach rechts benachbart und zugleich reducirt ist, so ist die Form $('a, 'b, a)$ ebenfalls reducirt und der Form (a, b, a') nach links benachbart. Da wir nun gesehen haben, dass eine reducirte Form (a', b, a) immer eine und nur eine nach rechts benachbarte reducirte Form $(a, 'b, 'a)$ hat, so folgt:

Jede reducirte Form (a, b, a') besitzt stets eine und nur eine nach links benachbarte reducirte Form $('a, 'b, a)$.

§. 78.

Aus den soeben bewiesenen Sätzen über die nach rechts und links benachbarten reducirten Formen ergiebt sich, dass man sämmtliche reducirte Formen einer positiven Determinante D in *Perioden**) eintheilen kann, die auf folgende Weise zu bilden sind. Man wähle irgend eine reducirte Form φ_0 und bilde die nach rechts und links fortgesetzte Reihe

$$\ldots \varphi_{-2}, \varphi_{-1}, \varphi_0, \varphi_1, \varphi_2 \ldots$$

der successiven nach rechts und nach links benachbarten reducirten Formen, welche durch das eine Glied φ_0 vollständig bestimmt sind. Da es nur eine endliche Anzahl von reducirten Formen der Determinante D giebt, und die ersten Coefficienten zweier auf einander folgenden Formen stets entgegengesetzte Zeichen haben, so muss einmal auf eine Form φ_μ dieser Reihe nach einer geraden Anzahl $2n$ von Gliedern eine mit φ_μ identische Form $\varphi_{\mu+2n}$ folgen; und da eine Form φ_μ oder $\varphi_{\mu+2n}$ nur eine

*) *Gauss: D. A.* art. 186.

einzige nach rechts, und nur eine einzige nach links benachbarte reducirte Form besitzt, so müssen auch die beiden Formen $\varphi_{\mu+1}$ und $\varphi_{\mu+1+2n}$, ebenso die beiden Formen $\varphi_{\mu-1}$ und $\varphi_{\mu-1+2n}$, und also auch allgemein je zwei Formen dieser Reihe identisch sein, deren Indices dieselbe Differenz $2n$ haben. In der ganzen Reihe sind daher höchstens $2n$ verschiedene Formen

$$\varphi_0,\ \varphi_1,\ \varphi_2 \ldots \varphi_{2n-2},\ \varphi_{2n-1};$$

und diese werden in der That alle von einander verschieden sein, wenn keine der Formen $\varphi_2,\ \varphi_4 \ldots \varphi_{2n-2}$ mit φ_0 identisch ist; denn wären φ_ν und $\varphi_{\nu+2n'}$ zwei identische Formen, so müsste auch $\varphi_{2n'}$ mit φ_0 identisch sein. Nehmen wir also an, dass $2n$ die Anzahl der wirklich verschiedenen Formen dieser Reihe ist, so besteht dieselbe aus einer nach beiden Seiten sich unendlich oft periodisch wiederholenden Folge dieser $2n$ Formen; je zwei Formen φ_μ und φ_ν, deren Indices eine durch $2n$ theilbare Differenz $\mu - \nu$ haben, sind identisch; und umgekehrt, sind die Formen φ_μ und φ_ν identisch, so ist $\mu \equiv \nu$ (mod. $2n$).

Es kann nun sein, dass diese $2n$ Formen alle reducirten Formen der Determinante D erschöpfen; aber es ist auch möglich, dass ausser ihnen noch andere reducirte Formen derselben Determinante existiren. Im letztern Fall sei ψ_0 eine solche, in der obigen Periode nicht enthaltene reducirte Form, so entspricht ihr ebenso eine Periode von $2m$ unter einander verschiedenen Formen

$$\psi_0,\ \psi_1,\ \psi_2 \ldots \psi_{2m-2},\ \psi_{2m-1};$$

alle diese Formen der zweiten Periode werden auch von denen der ersten verschieden sein; denn besässen beide Perioden eine gemeinschaftliche Form, so wären beide Reihen vollständig identisch, da von dieser gemeinschaftlichen Form aus die Reihe nur auf eine einzige Weise nach rechts und links fortgesetzt werden kann.

In derselben Weise kann man fortfahren, bis endlich alle reducirten Formen in verschiedene Perioden eingetheilt sind; die Anzahl der Perioden ist nothwendig eine endliche; die Anzahl der Glieder kann in verschiedenen Perioden verschieden sein, jedenfalls ist sie stets gerade*).

---

*) Von besonderem Interesse sind noch folgende Bemerkungen (*Gauss: D. A.* artt. 187, 194). Wenn (a, b, c) eine reducirte Form ist, so gilt Dasselbe von ihrem Gefährten (c, b, a) (§. 74); sind die Perioden dieser beiden Formen entwickelt, und die beiden Formen selbst nach den Plätzen, welche sie in diesen Perioden einnehmen, mit φ_μ und ψ_ν bezeichnet, so leuchtet

Beispiel 1: Wir haben (§. 75) das System der reducirten Formen für die Determinante $D = 13$ aufgestellt; nehmen wir z. B. für φ_0 die Form $(3, 1, -4)$, so erhalten wir folgende Periode von zehn Formen

$$\varphi_0 = (3, 1, -4);\ \varphi_1 = (-4, 3, 1);$$
$$\varphi_2 = (1, 3, -4);\ \varphi_3 = (-4, 1, 3);$$
$$\varphi_4 = (3, 2, -3);\ \varphi_5 = (-3, 1, 4);$$
$$\varphi_6 = (4, 3, -1);\ \varphi_7 = (-1, 3, 4);$$
$$\varphi_8 = (4, 1, -3);\ \varphi_9 = (-3, 2, 3).$$

---

ein, dass auch $\varphi_{\mu+1}$ und $\psi_{\nu-1}$, allgemeiner je zwei Formen $\varphi_{\mu+h}$ und $\psi_{\nu-h}$ Gefährten sind, wo h jede beliebige ganze Zahl bedeutet. Hieraus geht hervor, dass beide Perioden aus gleich vielen Gliedern bestehen werden.

Es ist nun möglich, dass beide Perioden identisch sind, dass also ψ_ν selbst ein Glied in der Periode der Form φ_μ ist; und dann wird offenbar der Gefährte einer jeden Form dieser Periode ein Glied derselben Periode sein. Ist nun φ_r der Gefährte von φ_0, so ist, weil die äusseren Coefficienten einer reducirten Form entgegengesetzte Vorzeichen, und ausserdem die ersten Coefficienten der auf einander folgenden Formen abwechselnde Vorzeichen haben, nothwendig r ungerade $= 2m - 1$; da nun φ_0 und φ_{2m-1} Gefährten sind, so gilt Dasselbe von φ_h und φ_{2m-1-h}, also auch von φ_m und φ_{m-1}, und ebenso, wenn $2n$ die Anzahl der Glieder der Periode bedeutet, von φ_{m+n} und $\varphi_{m-1-n} = \varphi_{m+n-1}$; bezeichnet man daher irgend eine der beiden Formen φ_m oder φ_{m+n} mit (A, B, C), so ist die ihr nach links benachbarte Form identisch mit (C, B, A), und folglich ist $2B \equiv 0 \pmod{A}$, d. h. φ_m und φ_{m+n} sind **ambige** Formen; und sie sind verschieden, weil m nicht $\equiv m + n \pmod{2n}$ ist.

Umgekehrt, ist in einer Periode eine ambige Form (A, B, C) enthalten, so ist ihr linker Nachbar ihr Gefährte (C, B, A), und folglich findet sich in derselben Periode noch eine zweite ambige Form. Ausser diesen beiden ambigen Formen φ_m und φ_{m+n} giebt es aber keine andere ambige Form in derselben Periode; denn, wenn φ_s eine ambige Form ist, so sind φ_{s-1} und φ_s, und folglich auch φ_{2s-1} und φ_0 Gefährten; mithin ist φ_{2s-1} identisch mit φ_{2m-1}, folglich $2s \equiv 2m \pmod{2n}$, also $s \equiv m$, oder $s \equiv m + n \pmod{2n}$.

Dieser Fall kann offenbar nur bei der Periode einer solchen Form eintreten (§§. 56, 58), welche ihrem Gefährten eigentlich und folglich sich selbst uneigentlich äquivalent ist, d. h. wenn die Form einer sogenannten **ambigen Classe** angehört. Dass umgekehrt jedes Mal, wenn diese Bedingung erfüllt ist, die Periode der Form auch ihren Gefährten und folglich zwei ambige Formen enthalten muss, ist eine unmittelbare Folge des weiter unten (§. 82) bewiesenen Hauptsatzes dieser ganzen Theorie. — Man vergleiche die Beispiele im Text.

Diese Rechnung geschieht am einfachsten auf folgende Art; um aus der reducirten Form (a, b, a') die ihr nach rechts benachbarte reducirte Form (a', b', a'') zu finden, braucht man nur ihren mittlern Coefficienten b' zu suchen, welcher durch die Bedingung $b' = -b - a'\delta \equiv -b$ (mod. a') und die Nebenbedingungen

$$\lambda + 1 - (a') \leqq b' \leqq \lambda$$

stets vollständig bestimmt ist und durch den blossen Anblick der Form sogleich erkannt wird. In unserm Fall ist $\lambda = 3$; man findet daher den mittlern Coefficienten b' der Form φ_1 durch die Bedingungen

$$b' \equiv -1 \text{ (mod. 4)}, \quad 0 \leqq b' \leqq 3,$$

nämlich $b' = 3$. Und nachdem so b' und $\delta = 1$ gefunden sind, ergiebt sich

$$a'' = \frac{b'^2 - D}{a'} = a + (b - b')\delta,$$

also in unserm Fall $a'' = 1$. In derselben Weise ist fortzufahren, bis die erste Form φ_0 sich reproducirt; in unserm Beispiel wird der mittlere Coefficient von φ_{10} dadurch bestimmt, dass er $\equiv -2$ (mod. 3) sein, und ausserdem nicht ausserhalb der Grenzen 1 und 3 liegen muss, woraus folgt, dass er $= 1$ ist; also wird φ_{10} identisch mit φ_0.

Die so gefundenen zehn ursprünglichen Formen der ersten Art erschöpfen aber noch nicht alle reducirten Formen der Determinante 13; es bleiben noch zwei ursprüngliche Formen der zweiten Art übrig

$$\psi_0 = (2, 3, -2), \quad \psi_1 = (-2, 3, 2),$$

welche offenbar noch eine zweite Periode bilden.

Beispiel 2: Für $D = 19$ erhalten wir folgende zwei Perioden, jede von sechs Gliedern:

$$\varphi_0 = (3, 2, -5); \quad \varphi_1 = (-5, 3, 2)$$
$$\varphi_2 = (2, 3, -5); \quad \varphi_3 = (-5, 2, 3)$$
$$\varphi_4 = (3, 4, -1); \quad \varphi_5 = (-1, 4, 3)$$

und

$$\psi_0 = (-3, 2, 5); \quad \psi_1 = (5, 3, -2)$$
$$\psi_2 = (-2, 3, 5); \quad \psi_3 = (5, 2, -3)$$
$$\psi_4 = (-3, 4, 1); \quad \psi_5 = (1, 4, -3).$$

Beispiel 3: Für $D = 35$ erhält man folgende vier Perioden, jede von zwei Gliedern:

$$\varphi_0 = (\ 1, 5, -10), \quad \varphi_1 = (-10, 5, \ 1)$$
$$\psi_0 = (10, 5, -\ 1), \quad \psi_1 = (-\ 1, 5, 10)$$
$$\chi_0 = (\ 2, 5, -\ 5), \quad \chi_1 = (-\ 5, 5, \ 2)$$
$$\theta_0 = (\ 5, 5, -\ 2), \quad \theta_1 = (-\ 2, 5, \ 5).$$

Beispiel 4: Die 32 reducirten Formen der Determinante $D = 79$ zerfallen in vier Perioden von je sechs Gliedern und zwei Perioden von je vier Gliedern; eine der sechsgliedrigen Perioden ist folgende:

$$\varphi_0 = (7, 3, -10); \quad \varphi_1 = (-10, 7, 3)$$
$$\varphi_2 = (3, 8, -\ 5); \quad \varphi_3 = (-\ 5, 7, 6)$$
$$\varphi_4 = (6, 5, -\ 9); \quad \varphi_5 = (-\ 9, 4, 7);$$

aus ihr entstehen die drei anderen durch Vertauschung der äusseren Coefficienten (womit die Vertauschung von rechts nach links in der Folge der Glieder verbunden ist), ferner durch Verwandlung der Vorzeichen der äusseren Coefficienten in die entgegengesetzten. Eine der beiden viergliedrigen Perioden ist

$$\psi_0 = (1, 8, -15); \quad \psi_1 = (-15, 7, 2)$$
$$\psi_2 = (2, 7, -15); \quad \psi_3 = (-15, 8, 1);$$

aus ihr entsteht die andere durch die Zeichenänderung der äusseren Coefficienten.

§. 79.

Die vorhergehenden Untersuchungen über die Perioden der reducirten Formen von positiver Determinante stehen in der engsten Beziehung zu der Entwicklung der Wurzeln dieser Formen in Kettenbrüche. Nehmen wir für die Anfangsform φ_0 einer Periode immer eine solche, deren erster Coefficient *positiv* ist, so ist auch ihre *erste* Wurzel ω_0 positiv. Wir bezeichnen mit ω_μ die *erste* Wurzel der Form φ_μ, mit δ_μ den vierten Coefficienten der Substitution

$$\begin{pmatrix} 0, & +1 \\ -1, & \delta_\mu \end{pmatrix},$$

durch welche φ_μ in die nach rechts benachbarte Form $\varphi_{\mu+1}$ übergeht, und endlich mit k_μ den absoluten Werth von δ_μ. Da (nach §. 77) der Coefficient δ_μ seinem Zeichen nach mit ω_μ übereinstimmt, und dem absoluten Werth nach die grösste in dem absoluten Werth von ω_μ enthaltene ganze Zahl ist, und da die Wurzeln $\omega_0, \omega_1, \omega_2 \ldots$ abwechselnd positiv und negativ sind, so ist $(-1)^\mu \omega_\mu$ stets positiv, und folglich

$$k_\mu = (-1)^\mu \delta_\mu;$$

zwischen den successiven Wurzeln $\omega_\mu, \omega_{\mu+1} \ldots$ bestehen aber folgende Relationen (§. 77):

$$\omega_\mu = \delta_\mu - \frac{1}{\omega_{\mu+1}}; \quad \omega_{\mu+1} = \delta_{\mu+1} - \frac{1}{\omega_{\mu+2}} \cdots$$

multiplicirt man diese Gleichungen der Reihe nach mit ± 1, ∓ 1 u. s. w. der Art, dass die linke Seite stets positiv wird, so erhält man

$$\pm \omega_\mu = k_\mu + \frac{1}{\mp \omega_{\mu+1}}; \quad \mp \omega_{\mu+1} = k_{\mu+1} + \frac{1}{\pm \omega_{\mu+2}} \cdots$$

und hieraus ergiebt sich für den positiven irrationalen unechten Bruch $(-1)^\mu \omega_\mu$ der folgende unendliche Kettenbruch (§. 23):

$$(-1)^\mu \omega_\mu = (k_\mu, k_{\mu+1}, k_{\mu+2} \ldots).$$

Offenbar ist dieser Kettenbruch periodisch; denn besteht die Periode der reducirten Formen φ aus $2n$ Gliedern, so ist $\delta_{\mu+2n} = \delta_\mu$ und also auch $k_{\mu+2n} = k_\mu$; es wiederholt sich daher die Reihe der Zahlen k immer nach höchstens $2n$ Gliedern von Neuem.

Beispiel 1: Nehmen wir $D = 13$, so haben wir, um die erste Wurzel ω_0 der Form $\varphi_0 = (3, 1, -4)$ in einen Kettenbruch zu entwickeln, ihre Periode aufzustellen (§. 78):

$$\varphi_0 = (3, 1, -4); \quad \varphi_1 = (-4, 3, 1)$$
$$\varphi_2 = (1, 3, -4); \quad \varphi_3 = (-4, 1, 3)$$
$$\varphi_4 = (3, 2, -3); \quad \varphi_5 = (-3, 1, 4)$$
$$\varphi_6 = (4, 3, -1); \quad \varphi_7 = (-1, 3, 4)$$
$$\varphi_8 = (4, 1, -3); \quad \varphi_9 = (-3, 2, 3);$$

die successiven Werthe der Substitutionscoefficienten δ sind folgende:

$$\delta_0 = +1, \quad \delta_1 = -6, \quad \delta_2 = +1, \quad \delta_3 = -1, \quad \delta_4 = +1,$$
$$\delta_5 = -1, \quad \delta_6 = +6, \quad \delta_7 = -1, \quad \delta_8 = +1, \quad \delta_9 = -1;$$

daraus ergeben sich die absoluten Werthe

$$k_0 = 1,\quad k_1 = 6,\quad k_2 = 1,\quad k_3 = 1,\quad k_4 = 1,$$
$$k_5 = 1,\quad k_6 = 6,\quad k_7 = 1,\quad k_8 = 1,\quad k_9 = 1.$$

Hier zeigt sich die eigenthümliche Erscheinung, dass die Periode des Kettenbruchs nur aus fünf Gliedern besteht, während die Periode der Formen doppelt so viele Glieder enthält; wir werden später (§. 83) darauf zurückkommen. Die gesuchte Kettenbruch-Entwicklung ergiebt sich hieraus als die folgende:

$$\frac{1+\sqrt{13}}{4} = (1, 6, 1, 1, 1;\ 1, 6, 1, 1, 1;\ \ldots)$$

Ebenso liefern die beiden anderen reducirten Formen derselben Determinante $D = 13$, nämlich

$$\varphi_0 = (2, 3, -2),\quad \varphi_1 = (-2, 3, 2)$$

folgende Werthe

$$\delta_0 = +3,\ \delta_1 = -3,$$

also

$$k_0 = 3,\qquad k_1 = 3$$

und folglich

$$\frac{3+\sqrt{13}}{2} = (3;\ 3;\ \ldots);$$

auch hier ist die Periode des Kettenbruchs nur halb so gross wie die der reducirten Formen.

Beispiel 2: Für $D = 19$ giebt die sechsgliedrige Formenperiode

$$\varphi_0 = (3, 2, -5);\quad \varphi_1 = (-5, 3, 2)$$
$$\varphi_2 = (2, 3, -5);\quad \varphi_3 = (-5, 2, 3)$$
$$\varphi_4 = (3, 4, -1);\quad \varphi_5 = (-1, 4, 3)$$

die Zahlen

$$\delta_0 = +1,\ \delta_1 = -3,\ \delta_2 = +1,\ \delta_3 = -2,\ \delta_4 = +8,\ \delta_5 = -2;$$
$$k_0 = 1,\quad k_1 = 3,\quad k_2 = 1,\quad k_3 = 2,\quad k_4 = 8,\quad k_5 = 2;$$

also

$$\frac{2+\sqrt{19}}{5} = (1, 3, 1, 2, 8, 2;\ \ldots)$$

Beispiel 3: Für $D = 79$ giebt die sechsgliedrige Periode

$$\varphi_0 = (7, 3, -10); \quad \varphi_1 = (-10, 7, 3)$$
$$\varphi_2 = (3, 8, -5); \quad \varphi_3 = (-5, 7, 6)$$
$$\varphi_4 = (6, 5, -9); \quad \varphi_5 = (-9, 4, 7)$$

die Zahlen

$$\delta_0 = +1, \ \delta_1 = -5, \ \delta_2 = +3, \ \delta_3 = -2, \ \delta_4 = +1, \ \delta_5 = -1;$$
$$k_0 = 1, \quad k_1 = 5, \quad k_2 = 3, \quad k_3 = 2, \quad k_4 = 1, \quad k_5 = 1;$$

also entsteht die Entwicklung

$$\frac{3 + \sqrt{79}}{10} = (1, 5, 3, 2, 1, 1; \ldots).$$

Ebenso liefert die viergliedrige Periode

$$\varphi_0 = (1, 8, -15); \quad \varphi_1 = (-15, 7, 2)$$
$$\varphi_2 = (2, 7, -15); \quad \varphi_3 = (-15, 8, 1)$$

die Zahlen

$$\delta_0 = +1, \ \delta_1 = -7, \ \delta_2 = +1, \ \delta_3 = -16$$
$$k_0 = 1, \ k_1 = 7, \ k_2 = 1, \ k_3 = 16;$$

also den Kettenbruch

$$\frac{8 + \sqrt{79}}{15} = (1, 7, 1, 16; \ldots).$$

Zu gleicher Zeit findet man natürlich auch die Entwicklung der Wurzeln der drei anderen Formen

$$-\frac{7 + \sqrt{79}}{2} = -(7, 1, 16, 1; \ldots)$$
$$\frac{7 + \sqrt{79}}{15} = (1, 16, 1, 7; \ldots)$$
$$-\frac{8 + \sqrt{79}}{1} = -(16, 1, 7, 1; \ldots)$$

durch einfache Verschiebung der Periode*).

*) Die Form $(1, 0, -D)$ ist der reducirten Form $\varphi_0 = (1, \lambda, \lambda^2 - D)$ äquivalent; die letzte Form der entsprechenden Periode ist offenbar $\varphi_{2n-1} = (\lambda^2 - D, \lambda, 1)$, und hieraus folgt eine Entwicklung von der Form

$$\frac{1}{\sqrt{D} - \lambda} = (k_0 \ldots k_{n-2}, k_{n-1}, k_{n-2} \ldots k_0, 2\lambda; \ldots)$$

und

$$\sqrt{D} = (\lambda; k_0 \ldots k_{n-2}, k_{n-1}, k_{n-2} \ldots k_0, 2\lambda; \ldots).$$

Eine ähnliche Entwicklung tritt jedes Mal auf, wenn in der Periode zwei ambige Formen vorkommen (§. 78).

§. 80.

Es bleibt nun noch die schwierigste Frage zu beantworten übrig, nämlich die, ob zwei reducirte Formen derselben Determinante, welche verschiedenen Perioden angehören, äquivalent sein können oder nicht. Dazu müssen wir eine Digression über die Theorie der Kettenbrüche machen, in welcher wir einige weniger bekannte Sätze über dieselben beweisen wollen.

Ein Kettenbruch $(a, b, c, d \ldots)$, dessen sämmtliche Elemente $a, b, c, d \ldots$ positive ganze Zahlen sind (mit Ausnahme des ersten a, für welches auch der Werth Null gestattet ist), soll im Folgenden ein *regelmässiger* heissen; der Werth eines solchen endlichen oder unendlichen Kettenbruchs ist bekanntlich stets positiv, und umgekehrt ist bekannt, dass jeder positive Werth stets und nur auf eine einzige Weise in einen regelmässigen Kettenbruch verwandelt werden kann. Sehr wichtig für unsere Zwecke ist nun die Umwandlung eines *unregelmässigen* unendlichen Kettenbruchs

$$(\alpha, \beta, \gamma \ldots \mu, \nu, p, q, r \ldots u, v \ldots),$$

dessen Elemente ganze Zahlen und zwar von einem bestimmten p ab sämmtlich *positive* ganze Zahlen sind, in einen regelmässigen. Es wird sich zeigen, *dass bei dieser Umwandlung alle Elemente $u, v \ldots$ von einem bestimmten, in endlicher Entfernung liegenden, Element u ab unverändert bleiben, und dass die Differenz zwischen der Anzahl der geänderten und der Anzahl der sie ersetzenden Elemente eine gerade oder ungerade Zahl ist, je nachdem der Werth des ganzen Kettenbruchs positiv oder negativ ist.*

Um dies zu beweisen, nehmen wir an, es sei ν das letzte nicht positive Element des Kettenbruchs, und wir setzen ausserdem zunächst voraus, dass ν nicht das erste Element des ganzen Kettenbruchs ist. Wir suchen nun die Unregelmässigkeit des Kettenbruchs von dieser äussersten Stelle ν zu entfernen und um mindestens eine Stelle weiter nach links zu drängen.

Hierzu brauchen wir offenbar nur den unendlichen Kettenbruch $(\mu, \nu, p, q \ldots)$ zu betrachten, den wir auch in endlicher Form (μ, ν, p') oder (μ, ν, p, q') oder (μ, ν, p, q, r') u. s. w. schreiben können, wenn wir die unendlichen regelmässigen Kettenbrüche

$$(p, q, r, s\ldots),\quad (q, r, s\ldots),\quad (r, s\ldots) \text{ u. s. w.}$$

zur Abkürzung mit p', q', r' u. s. w. bezeichnen. Wir haben nun folgende Fälle zu unterscheiden.

1. Ist $\nu = 0$, so ist

$$(\mu, 0, p') = \mu + p' = \mu + p + \frac{1}{q'}$$

oder also

$$(\mu, 0, p, q') = (\mu + p, q');$$

es ist also die Unregelmässigkeit von der Stelle $\nu = 0$ um mindestens eine Stelle nach links gedrängt, und zugleich ist an Stelle der abgeänderten drei Elemente $\mu, 0, p$ das einzige Element $\mu + p$ getreten.

2. Ist ν negativ $= -n$, und $n > 1$, so erhält man mit Benutzung der Identität

$$(g, -h) = (g - 1, 1, h - 1)$$

folgende successive Umformung:

$$(\mu, -n, p') = \left(\mu, -n + \frac{1}{p'}\right) = \left(\mu - 1, 1, n - 1 - \frac{1}{p'}\right)$$
$$= (\mu - 1, 1, n - 1, -p')$$

und hieraus durch nochmalige Anwendung derselben Identität

$$(\mu, -n, p, q') = (\mu - 1, 1, n - 2, 1, p' - 1)$$
$$= (\mu - 1, 1, n - 2, 1, p - 1, q').$$

An Stelle der drei abgeänderten Elemente μ, $-n$, p sind die fünf Elemente $\mu - 1$, 1, $n - 2$, 1, $p - 1$ getreten, und von diesen ist höchstens das erste negativ. Sollte ferner $n - 2$ oder $p - 1$, oder sollten beide Zahlen $= 0$ sein, so wird man durch einmalige oder zweimalige Anwendung der unter 1. aufgestellten Regel alle Elemente, mit Ausnahme des ersten, in positive verwandeln; auch dann wird der Unterschied zwischen der Anzahl der abgeänderten und der Anzahl der dieselben ersetzenden Elemente eine gerade Zahl bleiben, und die Unregelmässigkeit ist mindestens um eine Stelle nach links verschoben.

3. Ist $\nu = -1$, so ist die eben angegebene Regel nicht anwendbar; wenn gleichzeitig $p > 1$, so findet man

$$(\mu, -1, p, q') = (\mu - 2, 1, p - 2, q');$$

sollte $p = 2$ sein, so hat man wieder nach der unter 1. aufgestellten Regel zu verfahren. Ist aber $p = 1$, so hilft diese Formel Nichts; dann ist aber

$$(\mu, -1, 1, q') = \mu - 1 - q'$$

und folglich

$$(\mu, -1, 1, q, r, s') = (\mu - 2 - q, 1, r - 1, s');$$

und sollte $r = 1$ sein, so würde man wie in 1. verfahren.

Auf diese Weise ist in allen Fällen ohne Ausnahme die Unregelmässigkeit des Kettenbruchs von der Stelle ν um mindestens eine Stelle weiter nach links gedrängt, und zugleich ist der Unterschied zwischen der Anzahl der abgeänderten und der Anzahl der sie ersetzenden Elemente jedes Mal eine *gerade* Zahl. Durch successive Anwendung desselben Verfahrens wird man daher den ursprünglich gegebenen Kettenbruch

$$(\alpha, \beta, \gamma \ldots \mu, \nu, p, q, r \ldots t, u, v \ldots)$$

in einen andern

$$(\alpha', b, c \ldots k, l, u, v \ldots)$$

umformen können, in welchem alle auf das erste folgenden Elemente $b, c \ldots$ positive ganze Zahlen sind, welche von einer in endlicher Entfernung liegenden Stelle u an mit den Elementen des gegebenen Kettenbruchs übereinstimmen; und zwar wird der Unterschied zwischen der Anzahl der abgeänderten Elemente

$$\alpha, \beta, \gamma \ldots \mu, \nu, p, q, r \ldots t$$

und der Anzahl der sie ersetzenden Elemente

$$\alpha', b, c \ldots k, l$$

eine gerade Zahl sein, weil dasselbe bei jedem einzelnen Act der gesammten Umformung Statt findet.

Ist nun α' positiv oder $= 0$, so ist die Umformung vollendet, und der Werth des Kettenbruchs ist positiv; ist dagegen α' negativ $= -a$, so ist der Kettenbruch negativ, und zwar

$$= -(a - 1, 1, b - 1, c \ldots)$$

oder, wenn $b = 1$ sein sollte,

$$= -(a - 1, c + 1, d \ldots).$$

Bei diesem letzten Act ist die Anzahl der abgeänderten Elemente um eine Einheit kleiner oder grösser als die Anzahl der sie ersetzenden Elemente; und hiermit ist der letzte Punct unserer obigen Behauptung nachgewiesen.

§. 81.

Wir bedürfen zweitens für die Untersuchung der Aequivalenz zweier Formen noch des folgenden Satzes:

Sind α, β, γ, δ vier ganze Zahlen, welche der Bedingung

$$\alpha\delta - \beta\gamma = 1$$

genügen, und deren erste α von Null verschieden ist; findet ferner zwischen zwei Grössen ω und Ω die Relation

$$\omega = \frac{\gamma + \delta\Omega}{\alpha + \beta\Omega}$$

Statt; so kann man stets

$$\omega = (\gamma', m, n \ldots r, \beta', \Omega)$$

setzen, wo die Anzahl der positiven ganzen Zahlen $m, n \ldots r$ eine gerade ist, γ' und β' aber auch Null oder negative ganze Zahlen sein können.

Um diesen Satz zu beweisen, können wir, ohne die Allgemeinheit zu beeinträchtigen, annehmen, dass die von Null verschiedene ganze Zahl α *positiv* ist; denn sollte α negativ sein, so verwandele man die Zeichen aller vier Zahlen α, β, γ, δ in die entgegengesetzten, so bleibt die zwischen ihnen, und ebenso die zwischen ω und Ω bestehende Relation ungeändert. Ist nun zunächst $\alpha = 1$, also $\delta = \beta\gamma + 1$, so ist unmittelbar

$$\omega = \frac{\gamma + (\beta\gamma + 1)\Omega}{1 + \beta\Omega} = \gamma + \frac{\Omega}{1 + \beta\Omega} = (\gamma, \beta, \Omega),$$

also ist in diesem Fall unser Satz richtig. Ist aber $\alpha > 1$, so entwickle man den Bruch $\gamma : \alpha$ in den Kettenbruch $(\gamma', m, n \ldots r)$, dessen Elemente sämmtlich positive ganze Zahlen sind, mit Ausnahme des ersten γ', welches positiv, Null oder negativ sein wird, je nachdem γ positiv und grösser als α, oder positiv und kleiner als α, oder endlich negativ ist.

Wir können ferner voraussetzen, dass die Anzahl der positiven Elemente $m, n \ldots r$ gerade ist; denn da bei der gewöhnlichen Methode, einen Bruch $\gamma : \alpha$ in einen Kettenbruch zu verwandeln, das letzte Element r mindestens $= 2$ ist, so könnte man, wenn die Anzahl der Elemente $m, n \ldots r$ ungerade sein sollte, das letzte Element r in den Kettenbruch $r - 1 + \frac{1}{1}$ verwandeln und also statt

des obigen Kettenbruchs den folgenden $(\gamma', m, n \ldots r-1, 1)$ nehmen, in welchem die Anzahl der positiven Elemente $m, n \ldots r-1, 1$ nun gerade ist. Bildet man nun nach der früher (§. 23) angegebenen Methode die sogenannten Näherungsbrüche,

$$\frac{[\gamma']}{1}, \quad \frac{[\gamma', m]}{[m]}, \quad \frac{[\gamma', m, n]}{[m, n]} \ldots \frac{[\gamma', m, n \ldots q, r]}{[m, n \ldots q, r]},$$

so erkennt man leicht, dass ihre Nenner sämmtlich positiv sind. Damals haben wir auch bewiesen, dass diese Brüche irreductibel sind, und da der letzte der obigen Brüche dem in Folge der Relation $\alpha\delta - \beta\gamma = 1$ ebenfalls irreductibeln Bruche $\gamma : \alpha$ gleich, und α positiv ist, so muss

$$\alpha = [m, n \ldots q, r], \quad \gamma = [\gamma', m, n \ldots q, r]$$

sein, weil ein Bruch nur auf eine einzige Weise in die irreductibele Form mit positivem Nenner gebracht werden kann. Da ferner die Anzahl der Elemente $\gamma', m, n \ldots q, r$ ungerade ist, so folgt aus der damals aufgestellten Formel [§. 23, (9)], dass

$$[m, n \ldots q]\,[\gamma', m, n \ldots q, r] - [m, n \ldots q, r]\,[\gamma', m, n \ldots q] = -1$$

oder also

$$\alpha[\gamma', m, n \ldots q] - [m, n \ldots q]\gamma = 1$$

ist; vergleicht man dies mit der Relation $\alpha\delta - \beta\gamma = 1$, so ergiebt sich (ähnlich wie im §. 60), dass man

$$\delta = [\gamma', m, n \ldots q] + \gamma\beta'$$
$$\beta = [m, n \ldots q] + \alpha\beta'$$

d. h.

$$\delta = [\gamma', m, n \ldots q, r, \beta']$$
$$\beta = [m, n \ldots q, r, \beta']$$

also

$$\frac{\delta}{\beta} = (\gamma', m, n \ldots q, r, \beta')$$

setzen kann, wo β' eine ganze Zahl bedeutet*). Nach demselben Bildungsgesetz ist nun

$$\gamma + \delta\Omega = [\gamma', m, n \ldots r, \beta', \Omega]$$
$$\alpha + \beta\Omega = [m, n \ldots r, \beta', \Omega]$$

und folglich, wie zu beweisen war,

$$\omega = (\gamma', m, n \ldots r, \beta', \Omega).$$

*) Da die Brüche $\gamma : \alpha$, $\beta : \alpha$ resp. den Kettenbrüchen $(\gamma', m : \ldots r)$, $(\beta', r \ldots m)$ gleich sind, so sind γ', β' die grössten in denselben enthaltenen ganzen Zahlen (im Sinne des §. 43).

§. 82.

Nachdem auch dieser zweite Punct aus der Theorie der Kettenbrüche behandelt ist, schreiten wir zur definitiven Entscheidung der Frage, ob zwei verschiedene Perioden von reducirten Formen einer positiven Determinante äquivalente Formen enthalten können. Es seien daher (a, b, c) und (A, B, C) zwei reducirte (eigentlich) äquivalente Formen; da alle Formen einer und derselben Periode einander stets äquivalent sind, so können wir annehmen, dass die ersten Coefficienten a, A, und folglich auch die ersten Wurzeln dieser beiden Formen *positiv* sind, weil im entgegengesetzten Fall die unmittelbar benachbarten Formen diese Eigenschaft besitzen würden. Bezeichnen wir (a, b, c) mit φ_0 und (A, B, C) mit Φ_0, und bilden wir für jede dieser beiden Formen (nach §. 78) die sie enthaltende Periode, so erhalten wir dadurch für die ersten Wurzeln ω_0, Ω_0 dieser beiden Formen die regelmässigen Kettenbrüche

$$\omega_0 = (k_0, k_1, k_2 \ldots),$$
$$\Omega_0 = (K_0, K_1, K_2 \ldots).$$

Ist nun $\binom{\alpha, \beta}{\gamma, \delta}$ eine Substitution, durch welche φ_0 in Φ_0 übergeht, so besteht zwischen den ersten Wurzeln ω_0, Ω_0 die Relation

$$\omega_0 = \frac{\gamma + \delta\Omega_0}{\alpha + \beta\Omega_0},$$

und ausserdem ist

$$\alpha\delta - \beta\gamma = 1.$$

Da ferner α nicht $= 0$ sein kann, weil sonst $A = c$, also A negativ wäre, so kann man nach dem so eben bewiesenen Satze

$$\omega_0 = (\gamma', m, n \ldots r, \beta', \Omega_0)$$

und also auch

$$\omega_0 = (\gamma', m, n \ldots r, \beta', K_0, K_1, K_2 \ldots)$$

setzen, und in diesem unendlichen Kettenbruch, welcher wenigstens von der Stelle K_0 ab keine Unregelmässigkeit enthält, ist die Anzahl der Elemente $\gamma', m, n \ldots r, \beta'$ eine gerade $= 2g$. Ist β' positiv, so ist, da $\omega_0 > 1$ ist, auch γ' positiv, also der Bruch regelmässig. Ist aber $\beta' = 0$ oder negativ, so forme man den Kettenbruch nach den obigen Regeln (§. 80) in einen regelmässigen um; nimmt man μ hinreichend gross, so werden die Elemente $K_\mu, K_{\mu+1} \ldots$ bei

dieser Umformung ungeändert bleiben, und die Anzahl ν der Elemente, welche an die Stelle der vorhergehenden $(2g + \mu)$ Elemente

$$\gamma', m, n \ldots r, \beta', K_0 \ldots K_{\mu-1}$$

treten, wird $\equiv \mu$ (mod. 2) sein (nach §. 80), da der Werth des ganzen Kettenbruchs *positiv* ist. Da nun ω_0 nur auf eine einzige Weise als ein regelmässiger Kettenbruch dargestellt werden kann, so müssen die Zahlen

$$K_\mu, K_{\mu+1}, K_{\mu+2} \ldots\ldots$$

resp. mit den Zahlen

$$k_\nu, k_{\nu+1}, k_{\nu+2}, \ldots\ldots$$

identisch sein. Ist daher $\mu + h$ ein Multiplum von der Anzahl der Formen, welche die Periode der Form Φ_0 bilden, und also eine gerade Zahl, so ist auch $\nu + h$ eine gerade Zahl $= 2m$, und die Zahlen

$$K_{\mu+h}, K_{\mu+h+1}, K_{\mu+h+2} \ldots$$

stimmen mit den Zahlen

$$K_0, K_1, K_2 \ldots,$$

und diese folglich mit den Zahlen

$$k_{2m}, k_{2m+1}, k_{2m+2} \ldots$$

überein. Hieraus folgt unmittelbar

$$\Omega_0 = (k_{2m}, k_{2m+1} \ldots) = \omega_{2m};$$

und da durch ihre erste Wurzel auch stets die Form vollständig charakterisirt ist (§. 72), so schliessen wir hieraus, dass die Form Φ_0 mit der Form φ_{2m} identisch sein muss, dass also Φ_0 sich in der aus φ_0 entwickelten Periode befinden muss. Wir haben so folgenden *Hauptsatz**) gewonnen:

Zwei äquivalente reducirte Formen von positiver Determinante gehören einer und derselben Periode an; zwei reducirte Formen können nicht äquivalent sein, wenn sie verschiedenen Perioden angehören.

Mit Hülfe dieses Satzes ergiebt sich nun eine Methode, um zu prüfen, ob zwei gegebene Formen von gleicher positiver Determinante äquivalent sind oder nicht. Man suche (nach §. 76) zu jeder der beiden Formen eine ihr äquivalente reducirte Form; je nachdem die so gefundenen reducirten Formen derselben oder verschiedenen Perioden angehören, sind die gegebenen Formen

*) *Gauss: D. A.* art. 193.

äquivalent, oder nicht äquivalent. Im erstern Fall ergiebt sich offenbar zugleich eine Substitution, durch welche die eine Form in die andere übergeht (vergl. §. 66).

Beispiel: Die beiden gegebenen Formen seien (713, 60, 5) und (62, 95, 145), welche dieselbe Determinante $D = 35$ haben. Die erste geht durch die Substitution $\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix}$ in die reducirte Form (5, 5, — 2), die zweite durch die Substitution $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$ in die reducirte Form (— 2, 5, 5) über (§. 76). Diese beiden reducirten Formen gehören aber derselben zweigliedrigen Periode (5, 5, — 2), (— 2, 5, 5) an, und zwar geht die erstere durch die Substitution $\begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix}$ in die letztere über. Mithin sind die beiden gegebenen Formen (713, 60, 5) und (62, 95, 145) äquivalent, und da $\begin{pmatrix} -7, & -10 \\ -2, & -3 \end{pmatrix}$ die inverse Substitution von $\begin{pmatrix} -3, & +10 \\ +2, & -7 \end{pmatrix}$ ist, so geht die erstere dieser beiden Formen durch die Substitution $\begin{pmatrix} 0, & +1 \\ -1, & -13 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix} \begin{pmatrix} -7, & -10 \\ -2, & -3 \end{pmatrix} = \begin{pmatrix} -3, & -5 \\ +41, & +68 \end{pmatrix}$ in die letztere über.

§. 83.

Durch unsere letzten Untersuchungen ist das erste der beiden in §. 59 aufgestellten Hauptprobleme auch für Formen von *positiver* Determinante gelöst; das zweite haben wir in §. 62 auf die Auflösung der unbestimmten Gleichung

$$t^2 - Du^2 = \sigma^2$$

zurückgeführt, und es bleibt daher, um in der Theorie der Formen von positiver Determinante zu demselben Abschluss zu kommen, wie früher für negative Determinanten, nur noch übrig, diese Gleichung für jeden positiven (nicht quadratischen) Werth der Determinante D vollständig aufzulösen. *Fermat* hat diese Gleichung den Mathematikern zuerst vorgelegt, worauf ihre Lösung von dem Engländer *Pell* angegeben wurde; allein obwohl seine Methode die Lösung in jedem Fall wirklich giebt, so lag doch in ihr nicht der Nachweis, dass sie immer zum Ziele führen muss, und dass die Gleichung ausser der evidenten Auflösung $t = \pm \sigma$, $u = 0$ noch andere Auflösungen besitzt. Diese Lücke ist erst von *Lagrange* *) ausgefüllt, und hierin besteht wohl eine der bedeutend-

*) *Solution d'un Problème d'Arithmétique*, Miscellanea Taurinensia, Tom. IV. (Œuvres de Lagrange, publ. par Serret, T. I. 1867. p. 669.) —

sten Leistungen des grossen Mathematikers auf dem Gebiete der Zahlentheorie, da die von ihm zu diesem Zweck eingeführten Principien in hohem Grade der Verallgemeinerung fähig und deshalb auch auf ähnliche höhere Probleme anwendbar sind *).

Wir schlagen hier einen ganz andern Weg ein, der sich den zunächst vorangehenden Untersuchungen unmittelbar anschliesst. Der Zusammenhang zwischen der obigen unbestimmten Gleichung und dem zweiten Hauptproblem in der Theorie der Aequivalenz war folgender. Ist (a, b, c) eine Form von der Determinante D und vom Theiler σ, und ist $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ irgend eine eigentliche Substitution, durch welche (a, b, c) in sich selbst übergeht so ist stets

$$\alpha = \frac{t - bu}{\sigma}, \quad \beta = -\frac{cu}{\sigma}, \quad \gamma = \frac{au}{\sigma}, \quad \delta = \frac{t + bu}{\sigma},$$

wo t, u zwei der Gleichung

$$t^2 - Du^2 = \sigma^2$$

genügende ganze Zahlen bedeuten; und umgekehrt, jeder Auflösung t, u der unbestimmten Gleichung entspricht durch die vorstehenden Formeln eine Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$, durch welche die Form (a, b, c) in sich selbst übergeht. Wir haben nun durch die letzten Untersuchungen, wie sich gleich zeigen wird, ein Mittel gewonnen, alle Transformationen $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ einer reducirten Form von positiver Determinante D in sich selbst direct zu finden, und folglich können wir hieraus auch alle Auflösungen t, u der unbestimmten Gleichung ableiten. Wir schicken der Ausführung dieser Untersuchung noch eine Bemerkung über die Perioden der reducirten Formen voraus.

Wir wissen, dass die Reihe der positiven Zahlen k, welche die Elemente des Kettenbruchs bilden, in den die erste Wurzel ω_0

Sur la solution des problèmes indéterminés du second degré, Mém. de l'Ac. de Berlin T. XXIII. (Œuvres de L. T. II. 1868. p. 375.) — *Additions aux Elémens d'Algèbre par L. Euler* §§. II, VIII. — Das Verdienst, die tiefe Bedeutung der Pell'schen Gleichung für die allgemeine Auflösung der unbestimmten Gleichungen zweiten Grades zuerst dargethan zu haben, gebührt *Euler*; man vergl.: *De solutione problematum Diophanteorum per numeros integros*, Comm. Petrop. VI. p. 175. *De resolutione formularum quadraticarum indeterminatarum per numeros integros*, Nov. Comm. Petrop. IX. p. 3. *De usu novi algorithmi in problemate Pelliano solvendo*, Nov. Comm. Petrop. XI. p. 28. *Nova subsidia pro resolutione formulae* $axx + 1 = yy$, Opusc. anal. I. p. 310. — Man vergleiche ferner *Gauss*: *D. A.* artt. 197 — 202.

*) Siehe Supplement VIII.

einer reducirten Form φ_0 entwickelt wird, eine gerade Anzahl von Gliedern

$$k_0, \; k_1 \ldots k_{2n-1}$$

enthält, nach welchen dieselben Glieder periodisch wiederkehren; und zwar ist diese Anzahl $2n$ die der reducirten Formen, welche mit φ_0 in einer Periode enthalten sind. Wir haben aber oben (§. 79) an einzelnen Beispielen gesehen, dass die Zahlen k aus kleineren Perioden bestehen können; wir fanden z. B. aus der zehngliedrigen Formenperiode der Determinante $D = 13$ folgende Zahlen:

$$\delta_0 = +1, \quad \delta_1 = -6, \quad \delta_2 = +1, \quad \delta_3 = -1, \quad \delta_4 = +1;$$
$$\delta_5 = -1, \quad \delta_6 = +6, \quad \delta_7 = -1, \quad \delta_8 = +1, \quad \delta_9 = -1;$$

und also

$$k_0 = 1, \quad k_1 = 6, \quad k_2 = 1, \quad k_3 = 1, \quad k_4 = 1;$$

und hierauf wiederholt sich schon dieselbe Reihe

$$k_5 = 1, \quad k_6 = 6, \quad k_7 = 1, \quad k_8 = 1, \quad k_9 = 1.$$

Es ist nun wichtig zu untersuchen, wann dies eintreten kann. Es sei daher $2n$ die Gliederanzahl der Formenperiode und m die Gliederanzahl irgend einer Periode in der Reihe der Zahlen k. Dann ist, indem wir die früheren Bezeichnungen für die Formen und ihre ersten Wurzeln beibehalten, wenn m gerade ist,

$$\omega_m = (k_m, k_{m+1} \ldots) = (k_0, k_1 \ldots)$$

und folglich $\omega_m = \omega_0$, und also auch φ_m identisch mit φ_0 und daher nothwendig m ein Multiplum von $2n$; es existirt also jedenfalls keine kleinere Periode von gerader Gliederanzahl als die der ganzen Formenperiode entsprechende. Ist dagegen m ungerade, so ist $2m$ ebenfalls die Gliederanzahl einer Periode in der Reihe der Zahlen k, und folglich ist nach dem eben Bewiesenen $2m$ ein Multiplum von $2n$, also m mindestens $= n$; der Fall, dass die Periode der Zahlen k kürzer ist als die aus $2n$ Gliedern bestehende Periode der Formen, kann also nur dann eintreten, wenn n eine *ungerade* Zahl ist, indem dann, wie wir ja auch an dem obigen Beispiel sehen, die Periode der Zahlen k aus n Gliedern bestehen kann; es ist dann $\omega_n = -\omega_0$, und also $c_n = -c_0$, $b_n = b_0$, $a_n = -a_0$. Doch muss man sich hüten zu glauben, dass diese Erscheinung jedesmal wirklich eintreten *muss*, wenn n ungerade ist; denn wir haben nur gezeigt, dass sie in diesem Fall allein eintreten *kann*. Für $D = 19$ z. B. sind die beiden Formenperioden

sechsgliedrig (§. 79), also ist $n = 3$; aber die Perioden der Zahlen k sind nicht dreigliedrig, sondern sechsgliedrig *).

*) Die Erscheinung, dass die Kettenbruch-Entwicklung nur halb so lang ist, als die Periode der Form, wird, wie oben gezeigt ist, nur dann eintreten, wenn die Formen (a, b, c) und $(-a, b, -c)$ äquivalent sind, und man erkennt leicht (aus §. 82), dass sie dann auch stets eintreten muss. Führt man nun die Untersuchung über die Aequivalenz dieser beiden Formen genau ebenso durch wie in §. 62, so erhält man das Resultat: Die Coefficienten einer jeden Substitution $\binom{\lambda,\ \mu}{\nu,\ \varrho}$, durch welche eine Form (a, b, c) von der Determinante D und vom Theiler σ in die Form $(-a, b, -c)$ übergeht, sind in den Formeln

$$\lambda = \frac{t - bu}{\sigma},\quad \mu = \frac{cu}{\sigma},\quad \nu = \frac{au}{\sigma},\quad \varrho = -\frac{t + bu}{\sigma} \qquad \text{(I)}$$

enthalten, wo t, u zwei ganze Zahlen bedeuten, welche der unbestimmten Gleichung

$$t^2 - Du^2 = -\sigma^2 \qquad \text{(II)}$$

Genüge leisten; und umgekehrt, giebt es zwei solche ganze Zahlen t, u, so liefern jene Formeln (I) stets eine Substitution von der angegebenen Beschaffenheit. Die erwähnte Erscheinung wird daher stets und nur dann auftreten, wenn die Gleichung (II) *möglich* ist; tritt sie daher in der Periode irgend einer Form auf, so wird sie auch in allen Perioden derjenigen Formen auftreten, welche zu derselben *Ordnung* gehören (§. 61); ist ferner die Gleichung $t^2 - Du^2 = -1$ möglich, so wird sie bei allen Perioden dieser Determinante D auftreten. Dies ist z. B. stets der Fall, wenn $D = p^{2s+1}$ und p eine positive Primzahl $\equiv 1 \pmod{4}$ ist; denn sind T, U die *kleinsten* positiven Zahlen, welche der Gleichung $T^2 - DU^2 = +1$ genügen (§. 84), so ist T ungerade, U gerade, und

$$\frac{T-1}{2} \cdot \frac{T+1}{2} = D\left(\frac{U}{2}\right)^2;$$

da die beiden Factoren linker Hand relative Primzahlen sind, so ist einer und nur einer von ihnen durch D theilbar; wäre nun $T - 1 = 2Df^2$, $T + 1 = 2g^2$, $U = 2fg$, so wäre $g^2 - Df^2 = +1$, und $f < U$, gegen die Voraussetzung; es muss daher $T - 1 = 2f^2$, $T + 1 = 2Dg^2$, $U = 2fg$, und also $f^2 - Dg^2 = -1$ sein, w. z. b. w. Zugleich leuchtet ein, dass $T + U\sqrt{D} = (f + g\sqrt{D})^2$ ist, was nur ein specieller Fall eines allgemeineren Satzes ist.

Besonders interessante Resultate erhält man, wenn man, falls die Gleichung (II) möglich ist, die Perioden von *ambigen* Formen betrachtet (§. 78). Um uns auf den einfachsten Fall zu beschränken, nehmen wir an, die Gleichung $t^2 - Du^2 = -1$ sei möglich; ist nun λ die grösste in $\sqrt{D}$ enthaltene ganze Zahl, also $\varphi_0 = (1, \lambda, \lambda^2 - D)$ eine reducirte und zugleich ambige Form, deren Periode $2n$ Glieder enthält (§. 79), so muss n ungerade $= 2m + 1$, und $\varphi_n = (-1, \lambda, D - \lambda^2)$, also $\varphi_{2m} = (D - \lambda^2, \lambda, -1)$ sein, und hieraus folgt leicht, dass $\varphi_m = (a, b, -a)$, $\varphi_{3m+1} = (-a, b, a)$, also $D = a^2 + b^2$ ist, wo a ungerade und relative Primzahl zu b ist, weil φ_0 eine ursprüngliche Form der ersten Art ist. Da wir vorhin gesehen haben, dass dieser

Um nun die unbestimmte Gleichung $t^2 - Du^2 = \sigma^2$ zu lösen, in welcher D eine beliebige nicht quadratische positive Zahl, und entweder $D \equiv 0$ (mod. σ^2), oder $4D \equiv \sigma^2$ (mod. $4\sigma^2$) ist, nehmen wir eine beliebige *reducirte* Form (a, b, c) von der Determinante D und vom Theiler σ. (Dass eine solche stets existirt, leuchtet aus §§. 61, 76 unmittelbar ein.) Wir nehmen ferner, was stets gestattet ist, *a positiv*, und folglich *c negativ* an; dann ist die erste Wurzel ω dieser Form positiv, und folglich

$$\omega = (k_0,\ k_1 \ldots k_{2hn-2},\ k_{2hn-1},\ \omega),$$

wo $2n$ die Gliederanzahl der Formenperiode, und h eine beliebige positive ganze Zahl ist. Setzt man nun

$$\frac{\gamma}{\alpha} = (k_0,\ k_1 \ldots k_{2hn-2});\quad \frac{\delta}{\beta} = (k_0,\ k_1 \ldots k_{2hn-1})$$

d. h. (nach §. 23)

$$\alpha = [k_1 \ldots k_{2hn-2}],\quad \beta = [k_1 \ldots k_{2hn-2},\ k_{2hn-1}],$$
$$\gamma = [k_0,\ k_1 \ldots k_{2hn-2}],\quad \delta = [k_0,\ k_1 \ldots k_{2hn-2},\ k_{2hn-1}],$$

so ist nach den schon öfter benutzten Sätzen $\alpha\delta - \beta\gamma = 1$ und

$$\alpha + \beta\omega = [k_1 \ldots k_{2hn-2},\ k_{2hn-1},\ \omega]$$
$$\gamma + \delta\omega = [k_0,\ k_1 \ldots k_{2hn-2},\ k_{2hn-1},\ \omega]$$

und folglich

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega} = (k_0,\ k_1 \ldots k_{2hn-2},\ k_{2hn-1},\ \omega) = \omega,$$

woraus unmittelbar folgt (§. 73), dass die Form (a, b, c) durch die Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ in sich selbst übergeht.

Setzt man daher für h der Reihe nach alle positiven ganzen Zahlen 1, 2, 3 ..., so erhält man durch die Zähler und Nenner der Näherungsbrüche vom Range $2hn - 1$ und $2hn$ jedesmal eine entsprechende Transformation $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ der Form (a, b, c) in sich selbst (wenn $n = 1$ ist und $h = 1$ genommen wird, hat man $\alpha = 1$, $\beta = k_1$, $\gamma = k_0$, $\delta = k_0 k_1 + 1$ zu setzen); die vier Coefficienten $\alpha, \beta, \gamma, \delta$ sind immer *positiv*, und da ausserdem mit wachsendem h auch nothwendig die Zähler und Nenner der Näherungsbrüche

---

Fall stets eintritt, wenn D eine Primzahl $\equiv 1$ (mod. 4) ist, so liegt hierin ein neuer Beweis des Fermat'schen Satzes (§. 68), und zugleich eine directe Methode, die Zerlegung einer solchen Primzahl D in zwei Quadrate aus der Entwicklung von $\sqrt{D}$ in einen Kettenbruch abzuleiten (vergl. *Gauss: D. A.* art. 265; *Legendre: Théorie des Nombres* 3me éd. Tom. I. §. VII. (52)). Dies Resultat steht in der engsten Beziehung zu der biquadratischen Hülfsgleichung, welche bei der Theilung des Kreises in D gleiche Theile auftritt.

beständig wachsen, so entsprechen zwei verschiedenen Werthen von h auch zwei verschiedene Substitutionen $\binom{\alpha,\ \beta}{\gamma,\ \delta}$.

Umgekehrt wollen wir nun zeigen, dass man auf diese Weise *alle* die Transformationen $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ der Form (a, b, c) in sich selbst erhält, in denen die vier Coefficienten α, β, γ, δ sämmtlich *positiv* sind. Denn es sei $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ eine solche Substitution, so ist (§. 73)

$$\alpha\delta - \beta\gamma = 1 \text{ und } \omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

also auch

$$\beta\omega^2 + (\alpha - \delta)\,\omega - \gamma = 0,$$

und zwar müssen dieser quadratischen Gleichung beide Wurzeln der Gleichung genügen. Da nun die eine zwischen 1 und $+\infty$, die andere zwischen -1 und 0 liegt, so muss die linke Seite dieser Gleichung für $\omega = 1$ negativ, für $\omega = -1$ positiv ausfallen; hieraus folgt, dass

$$\gamma + \delta > \alpha + \beta, \quad \beta + \delta > \alpha + \gamma$$

ist, wo die Ungleichheitszeichen die Gleichheit ausschliessen. Da wir beweisen wollen, dass $\gamma : \alpha$ und $\delta : \beta$ zwei auf einander folgende Näherungsbrüche eines regelmässigen Kettenbruchs $(k_0, k_1 \ldots)$ sind, so haben wir vor allem zu zeigen, dass $\gamma \geqq \alpha$ und $\delta > \gamma$ ist; dies ergiebt sich in der That aus den vorstehenden Ungleichungen. Wäre nämlich $\delta \leqq \gamma$, so würde aus der zweiten Ungleichung folgen, dass $\alpha < \beta$ und also auch $\alpha\delta < \beta\gamma$ sein müsste, während doch $\alpha\delta = \beta\gamma + 1$ ist; also ist gewiss $\delta > \gamma$. Wäre ferner $\gamma < \alpha$, also $\alpha = \gamma + \varrho$, wo ϱ eine positive ganze Zahl bedeutet, so würde aus der ersten Ungleichheit folgen, dass $\delta > \beta + \varrho$, also auch

$$\alpha\delta - \beta\gamma > (\beta + \gamma)\,\varrho + \varrho^2$$

wäre; dies ist aber wieder unmöglich, da die linke Seite $= 1$, die rechte aber mindestens $= 3$ ist, weil β, γ, ϱ positive ganze Zahlen bedeuten; also ist in der That $\gamma \geqq \alpha$.

Hieraus folgt nun weiter, dass man

$$\frac{\gamma}{\alpha} = (\gamma', m \ldots q, r)$$

setzen kann, wo die Elemente γ', $m \ldots q$, r sämmtlich positiv sind, und zwar kann man es so einrichten, dass ihre Anzahl ungerade ist, weil man eventuell wieder r in $r - 1 + \frac{1}{1}$ auflösen kann. Nehmen wir ferner zunächst an, dass $\alpha > 1$ ist, so ist auch $\gamma > \alpha$ und γ nicht theilbar durch α, und folglich enthält der Kettenbruch

mindestens drei Elemente. Bilden wir daher den unmittelbar vorausgehenden Näherungsbruch

$$\frac{\varphi}{f} = (\gamma', m \ldots q),$$

so folgt aus $\alpha\varphi - f\gamma = 1$ und $\alpha\delta - \beta\gamma = 1$, dass man wieder $\beta = f + \alpha\beta'$, $\delta = \varphi + \gamma\beta'$ setzen kann, und hierin wird β' eine *positive* ganze Zahl sein. Wäre nämlich $\beta' = 0$, so wäre $\delta = \varphi$, und da φ gewiss $< \gamma$ ist, so wäre $\delta < \gamma$, während doch $\delta > \gamma$ ist; wäre ferner β' negativ, so wäre auch δ negativ, gegen unsere Voraussetzung, dass $\alpha, \beta, \gamma, \delta$ positive ganze Zahlen sind. Es ist daher

$$\frac{\delta}{\beta} = (\gamma', m \ldots q, r, \beta')$$

und folglich, ähnlich wie früher,

$$\omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega} = (\gamma', m \ldots q, r, \beta', \omega),$$

wo nun die Anzahl der positiven Elemente $\gamma', m \ldots q, r, \beta'$ gerade ist*). In dem bisher ausgeschlossenen Fall $\alpha = 1$ erhält man ein ganz ähnliches Resultat, denn dann ist

$$\omega = \frac{\gamma + (\beta\gamma + 1)\omega}{1 + \beta\omega} = (\gamma, \beta, \omega).$$

Wir erhalten daher für ω stets einen regelmässigen periodischen Kettenbruch

$$\omega = (\gamma', m \ldots q, r, \beta'; \gamma', m \ldots)$$

in welchem die Anzahl der Glieder $\gamma', m \ldots q, r, \beta'$ eine gerade ist. Da nun ein Werth ω nur auf eine einzige Weise in einen regelmässigen Kettenbruch entwickelt werden kann, so müssen die Zahlen $\gamma', m \ldots$ der Reihe nach mit den Zahlen $k_0, k_1 \ldots$ übereinstimmen; und da wir uns oben überzeugt haben, dass jede Periode der Zahlen k, deren Gliederzahl gerade ist, entweder mit der Reihe der den sämmtlichen $2n$ Formen entsprechenden Zahlen k identisch ist oder aus einer mehrmaligen Wiederholung dieser kleinsten Periode von gerader Gliederanzahl besteht, so ist also $r = k_{2hn-2}$, $\beta' = k_{2hn-1}$, wo h irgend eine positive ganze Zahl bezeichnet, und folglich

*) Dasselbe ergiebt sich auch unmittelbar daraus, dass die grössten in den Brüchen $\gamma : \alpha$, $\beta : \alpha$ enthaltenen ganzen Zahlen γ', β' zufolge der obigen Ungleichungen positiv sind (vergl. §. 81).

$$\frac{\gamma}{\alpha} = (k_0, k \ldots k_{2hn-2}), \quad \frac{\delta}{\beta} = (k_0, k_1 \ldots k_{2hn-2}, k_{2hn-1})$$

was zu beweisen war.

Nachdem wir gezeigt haben, wie wir alle aus vier *positiven* Coefficienten bestehenden Transformationen der reducirten Form (a, b, c) in sich selbst finden können, deren erster Coefficient a *positiv* ist, brauchen wir nur noch einen Blick auf die obigen Formeln

$$\alpha = \frac{t - bu}{\sigma}, \quad \beta = -\frac{cu}{\sigma}, \quad \gamma = \frac{au}{\sigma}, \quad \delta = \frac{t + bu}{\sigma}$$

zu werfen, um sogleich zu erkennen, dass die hieraus resultirenden Auflösungen t, u der unbestimmten Gleichung stets aus zwei *positiven* Zahlen t, u bestehen. Für u folgt dies aus der dritten Formel; da ferner, wie wir gesehen haben, $\delta > \gamma$ und $\gamma \geqq \alpha$, also $\delta > \alpha$ ist, so ergiebt sich, dass auch t positiv ist. Das Umgekehrte ist ebenfalls richtig; sind t, u zwei positive der unbestimmten Gleichung genügende Zahlen, so besteht die aus denselben abgeleitete Substitution $\binom{\alpha, \beta}{\gamma, \delta}$ aus vier positiven Zahlen; denn da die Form (a, b, c) reducirt, also b positiv, und der Annahme nach a positiv, also c negativ ist, so sind zunächst β, γ, δ positiv; endlich ist $t^2 - b^2u^2 = \sigma^2 - acu^2$ positiv, folglich hat $t - bu$, also auch α, dasselbe Zeichen wie $t + bu$, nämlich das positive.

§. 84.

Wir können daher behaupten, dass alle aus zwei positiven Zahlen t, u bestehenden Auflösungen — und auf diese kommt es uns zunächst allein an — durch die Kettenbruchentwicklung der Wurzel ω der Form (a, b, c) gefunden werden, und zwar jede nur ein einziges Mal. Aus dem Anblick der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ geht aber hervor, dass die zusammengehörigen positiven Werthe t, u gleichzeitig wachsen und gleichzeitig abnehmen; dasselbe folgt auch aus der Natur der Zähler und Nenner der Näherungsbrüche; u, und folglich auch t, wird gleichzeitig mit γ, also auch mit der von uns mit h bezeichneten Zahl wachsen; nehmen wir $h = 1$, so wird die entsprechende Auflösung, die wir mit (T, U) bezeichnen wollen, aus den kleinsten Zahlen bestehen,

d. h. T wird die kleinste aller Zahlen t, und gleichzeitig wird U die kleinste aller Zahlen u sein (die Auflösung $t = \sigma$, $u = 0$ gehört natürlich nicht zu den positiven Auflösungen). Diese kleinste Auflösung T, U findet man daher sehr leicht durch Entwicklung einer Periode von reducirten Formen.

Beispiel 1: Nimmt man für die Determinante $D = 79$ die reducirte Form (7, 3, — 10), welche natürlich von der ersten Art ist, so erhält man (§. 79)

$$k_0 = 1,\ k_1 = 5,\ k_2 = 3,\ k_3 = 2,\ k_4 = 1,\ k_5 = 1;$$

die successiven Näherungsbrüche sind folgende:

$$\frac{1}{1},\ \frac{6}{5},\ \frac{19}{16},\ \frac{44}{37},\ \frac{63}{53},\ \frac{107}{90};$$

aus den beiden letzten ergiebt sich daher die Substitution $\binom{53,\ 90}{63,\ 107}$; will man nur die kleinste Auflösung der Gleichung $t^2 - Du^2 = \sigma^2$, so braucht man nur die Nenner der Näherungsbrüche bis $\beta = 90$, oder die Zähler derselben bis $\gamma = 63$ zu bilden, so findet man durch die Formeln $\beta\sigma = -cu$ oder $\gamma\sigma = au$ die kleinste der Zahlen u, nämlich $U = 9$, und hieraus das zugehörige $T = \sqrt{(\sigma^2 + DU^2)} = 80$. Statt dessen findet man T auch durch die Formel $\alpha\sigma + bU$ oder $\delta\sigma - bU$.

Nimmt man die reducirte Form (1, 8, — 15), so findet man folgende Zahlen (§. 79)

$$k_0 = 1,\ k_1 = 7,\ k_2 = 1,\ k_3 = 16;$$

also die Näherungsbrüche

$$\frac{1}{1},\ \frac{8}{7},\ \frac{9}{8},\ \frac{152}{135};$$

die beiden letzten liefern die Substitution $\binom{8,\ 135}{9,\ 152}$, und hieraus ergiebt sich wieder $U = 9$, $T = 80$, wie vorher.

Beispiel 2: Es sei $D = 13 \equiv 1$ (mod. 4); um die kleinste Auflösung der Gleichung $t^2 - 13u^2 = 4$ zu finden, nehmen wir die reducirte Form (2, 3, —2), so ist (§. 79)

$$k_0 = 3,\ k_1 = 3;$$

die Näherungsbrüche sind also $\frac{3}{1}$ und $\frac{10}{3}$; dadurch erhalten wir die Substitution $\binom{1,\ 3}{3,\ 10}$ und hieraus $U = 3$, $T = 11$.

§. 85.

Nachdem wir gezeigt haben, wie die kleinste positive Auflösung (T, U) der unbestimmten Gleichung immer gefunden werden kann, gehen wir dazu über, alle anderen Auflösungen (t, u) auf diese eine zurückzuführen. Der Bequemlichkeit halber wollen wir, wenn t, u irgend zwei (positive oder negative) der Gleichung $t^2 - Du^2 = \sigma^2$ genügende Zahlen sind, und $\sqrt{D}$ stets positiv genommen wird, die Ausdrücke

$$\frac{t + u\sqrt{D}}{\sigma}, \quad \frac{t - u\sqrt{D}}{\sigma}$$

die zu dieser Auflösung (t, u) gehörigen Factoren nennen und als *ersten* und *zweiten Factor* von einander unterscheiden; das Product beider ist stets $= 1$; sie haben daher immer gleiche Zeichen, und zwar das positive oder negative, je nachdem t positiv oder negativ ist; haben ferner t und u gleiche Zeichen, so ist der erste Factor numerisch grösser als der zweite, folglich ist dann der erste numerisch > 1, der zweite numerisch < 1; das Gegentheil findet Statt, wenn t und u entgegengesetzte Zeichen haben; und wenn $u = 0$ ist, sind beide Factoren $= \pm 1$. Ist also z. B. (t, u) eine aus zwei positiven Zahlen bestehende Auflösung, so ist ihr erster Factor ein positiver unechter Bruch; und umgekehrt, ist der erste Factor ein positiver unechter Bruch, so sind beide Zahlen t, u positiv.

Sind (t', u') und (t'', u'') irgend zwei identische oder verschiedene Auflösungen, so kann man

$$\frac{t' + u'\sqrt{D}}{\sigma} \cdot \frac{t'' + u''\sqrt{D}}{\sigma} = \frac{t + u\sqrt{D}}{\sigma}$$

setzen, wo (t, u) wieder eine Auflösung bedeutet. Denn entwickelt man das Product links und trennt das Rationale vom Irrationalen, so findet man

$$t = \frac{t't'' + Du'u''}{\sigma}, \quad u = \frac{t'u'' + u't''}{\sigma};$$

da ferner aus der obigen Gleichung unmittelbar durch Verwandlung von $\sqrt{D}$ in $-\sqrt{D}$ oder auch durch den blossen Anblick der Ausdrücke für t, u die andere Gleichung

$$\frac{t'-u'\sqrt{D}}{\sigma}\cdot\frac{t''-u''\sqrt{D}}{\sigma}=\frac{t-u\sqrt{D}}{\sigma}$$

folgt, so ergiebt sich durch Multiplication beider

$$t^2-Du^2=\sigma^2;$$

es braucht daher nur noch gezeigt zu werden, dass u eine ganze Zahl ist, weil dann aus der vorstehenden Gleichung von selbst folgt, dass t^2, also auch t eine ganze Zahl ist. Geht nun σ^2 in D, folglich auch in t'^2, t''^2 auf, so sind t', t'' theilbar durch σ, und folglich ist u eine ganze Zahl; ist aber $4D\equiv\sigma^2 \pmod{4\sigma^2}$, so folgt $(2t')^2 \equiv(\sigma u')^2 \pmod{4\sigma^2}$, hieraus $2t'\equiv\sigma u'$, und ebenso $2t''\equiv\sigma u'' \pmod{2\sigma}$, folglich $2(t'u''+u't'')\equiv 2\sigma u'u''\equiv 0 \pmod{2\sigma}$; mithin ist u auch jetzt eine ganze Zahl, w. z. b. w.

Dieser Satz lässt sich ohne Weiteres auf beliebig viele Auflösungen (t', u'), (t'', u''), (t''', u''') . . . ausdehnen: setzt man

$$\frac{t'+u'\sqrt{D}}{\sigma}\cdot\frac{t''+u''\sqrt{D}}{\sigma}\cdot\frac{t'''+u'''\sqrt{D}}{\sigma}\cdots=\frac{t+u\sqrt{D}}{\sigma},$$

so wird (t, u) stets wieder eine ganzzahlige Auflösung sein. Bestehen ferner alle jene Auflösungen aus zwei positiven Zahlen, so sind alle Factoren linker Hand positive unechte Brüche; dasselbe gilt also auch von dem ersten Factor der Auflösung (t, u), und folglich sind t, u zwei positive Zahlen.

Setzen wir alle die einzelnen Auflösungen (t', u'), (t'', u'') . . . identisch mit der kleinsten positiven Auflösung (T, U), so können wir

$$\left(\frac{T+U\sqrt{D}}{\sigma}\right)^n=\frac{t_n+u_n\sqrt{D}}{\sigma}$$

setzen, wo n eine beliebige positive ganze Zahl bedeutet, und es wird dann (t_n, u_n) jedesmal eine positive Auflösung werden; zugleich leuchtet ein, dass mit wachsendem Exponenten n der Werth der linker Hand stehenden Potenz eines unechten Bruchs, und folglich auch $t_n+u_n\sqrt{D}$ beständig wächst, so dass verschiedene Werthe von n auch verschiedene Auflösungen (t_n, u_n) liefern; und da die beiden Zahlen t_n, u_n entweder beide gleichzeitig wachsen, oder beide gleichzeitig abnehmen, so tritt offenbar das erstere oder letztere ein, je nachdem n wächst oder abnimmt.

Umgekehrt können wir zeigen, dass durch die vorstehende Formel in der That jede positive Auflösung (t, u) geliefert wird. Denn wäre der erste Factor einer solchen Auflösung keine genaue Potenz des ersten Factors der kleinsten Auflösung (T, U), so

müsste er, da beide positive unechte Brüche sind, zwischen zwei successiven Potenzen

$$\left(\frac{T+U\sqrt{D}}{\sigma}\right)^n \text{ und } \left(\frac{T+U\sqrt{D}}{\sigma}\right)^{n+1}$$

des letztern liegen, wo n mindestens $= 1$ ist. Dann wäre also

$$\frac{t_n+u_n\sqrt{D}}{\sigma} < \frac{t+u\sqrt{D}}{\sigma} < \frac{t_n+u_n\sqrt{D}}{\sigma} \cdot \frac{T+U\sqrt{D}}{\sigma},$$

und folglich, wenn man

$$\frac{t+u\sqrt{D}}{\sigma} \cdot \frac{t_n-u_n\sqrt{D}}{\sigma} = \frac{t'+u'\sqrt{D}}{\sigma}$$

setzt,

$$1 < \frac{t'+u'\sqrt{D}}{\sigma} < \frac{T+U\sqrt{D}}{\sigma};$$

es existirte daher eine positive Auflösung (t', u'), welche aus kleineren Zahlen t', u' bestände, als die kleinste Auflösung (T, U); was unmöglich ist.

Man findet daher alle aus zwei positiven Zahlen bestehenden Auflösungen durch die Formeln

$$\frac{t_n}{\sigma} = \frac{1}{\sigma^n}\left\{T^n + \frac{n(n-1)}{1.2}T^{n-2}U^2D + \cdots\right\}$$

$$\frac{u_n}{\sigma} = \frac{1}{\sigma^n}\left\{\frac{n}{1}T^{n-1}U + \frac{n(n-1)(n-2)}{1.2.3}T^{n-3}U^3D + \cdots\right\}$$

wenn man der Reihe nach für n alle positiven ganzen Zahlen setzt. Da nun ferner

$$\frac{t_n-u_n\sqrt{D}}{\sigma} = \left(\frac{T-U\sqrt{D}}{\sigma}\right)^n = \left(\frac{T+U\sqrt{D}}{\sigma}\right)^{-n}$$

ist, so ergiebt sich, dass durch die Formel

$$\frac{t_n+u_n\sqrt{D}}{\sigma} = \left(\frac{T+U\sqrt{D}}{\sigma}\right)^n$$

sämmtliche Auflösungen t_n, u_n gegeben sind, in welchen t_n positiv ist, wenn man für n alle ganzen positiven und negativen Zahlen setzt, indem $u_{-n} = -u_n$, $t_{-n} = t_n$ ist. Für $n = 0$ ergiebt sich ferner $t_0 = +\sigma$, $u_0 = 0$. Will man daher alle Auflösungen t, u ohne Ausnahme in eine Formel zusammendrängen, so braucht man nur

$$\frac{t+u\sqrt{D}}{\sigma} = \pm\left(\frac{T+U\sqrt{D}}{\sigma}\right)^n$$

zu setzen, und hierin jedes der beiden Vorzeichen mit jedem ganzzahligen Exponenten n zu combiniren. Dass auf diese Weise keine Auflösung übergangen, und jede nur einmal erzeugt wird, folgt unmittelbar daraus, dass unter den vier verschiedenen Auflösungen

$$(t, u), (t, -u), (-t, u), (-t, -u),$$

wenn u nicht $= 0$ ist, immer eine und nur eine aus zwei positiven Zahlen besteht.

Hiermit ist nun das zweite Hauptproblem der Lehre von der Aequivalenz auch für Formen von *positiver* Determinante vollständig gelöst. Wir sind durch die vollständige Auflösung der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ in den Stand gesetzt, alle Transformationen einer solchen Form in sich selbst, und folglich auch alle Transformationen einer Form in eine äquivalente aus einer einzigen gegebenen solchen Transformation zu finden (§§. 61, 62); mithin ist auch die Aufgabe, alle eigentlichen Darstellungen einer gegebenen Zahl durch eine gegebene Form von positiver Determinante zu finden, als vollständig gelöst anzusehen (§. 60).

Fünfter Abschnitt.

Bestimmung der Anzahl der Classen, in welche die binären quadratischen Formen von gegebener Determinante zerfallen.

§. 86.

Wir schreiten nun, nachdem die elementaren Theile der Theorie der quadratischen Formen behandelt sind, zu tieferen Untersuchungen, und namentlich zur *Bestimmung der Classenanzahl der nicht äquivalenten Formen von einer gegebenen Determinante**). Wir beschränken uns dabei auf *ursprüngliche Formen der ersten oder zweiten Art* (§. 61), ferner, wenn die Determinante *negativ* ist, auf die Formen mit *positiven äusseren Coefficienten*, da die Classenanzahl der anderen Formen offenbar genau ebenso gross ist (§. 64). Unter diesen Beschränkungen denken wir uns ein vollständiges Formensystem S der σten Art für die Determinante D gebildet (§. 59). Zur Bestimmung der Anzahl der in diesem System S enthaltenen Formen führt die Betrachtung

*) *G. Lejeune Dirichlet: Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*, Crelle's Journal XIX, XXI. — Vergl. *Gauss: D. A.* Additam. ad art. 306. X, und die nachgelassenen Abhandlungen: *De nexu inter multitudinem classium in quas formae binariae secundi gradus distribuuntur eorumque determinantem*, Gauss' Werke Bd. II. 1863.

und genaue Definition aller durch sie darstellbaren Zahlen. Da durch eine Form der zweiten Art nur gerade Zahlen dargestellt werden können, so bezeichnen wir, um beide Fälle zusammenzufassen, die darstellbaren Zahlen allgemein mit σm, und ausserdem beschränken wir uns auf die Betrachtung derjenigen, in welchen *m positiv, ungerade und relative Primzahl gegen die Determinante D* ist. Endlich beschränken wir uns vorläufig noch auf *eigentliche* Darstellungen, d. h. auf die Annahme, dass die beiden darstellenden Zahlen x, y relative Primzahlen sind (§. 60).

Um den Charakter dieser Zahlen m genau festzustellen, erinnern wir uns, dass die Determinante D quadratischer Rest von jeder darstellbaren Zahl σm, d. h. dass die Congruenz

$$z^2 \equiv D \pmod{\sigma m}$$

möglich ist (§. 60). Es können daher in der ungeraden Zahl m nur solche Primzahlen f aufgehen, für welche

$$\left(\frac{D}{f}\right) = 1$$

ist. Umgekehrt: enthält m nur solche Primzahlen f, und ist die Anzahl der verschiedenen unter ihnen $= \mu$ (wo der Fall $\mu = 0$ nicht ausgeschlossen bleibt), so ist D quadratischer Rest von m, also auch von σm, und die obige Congruenz hat genau 2^μ incongruente Wurzeln (§. 37). Ist n ein bestimmter Repräsentant einer bestimmten dieser Wurzeln, so können wir $n^2 - D = \sigma^2 m l$ setzen, wo l eine ganze Zahl bedeutet (denn wenn $\sigma = 2$, also $D \equiv 1$ (mod. 4) ist, so ist n ungerade, also $n^2 - D$ durch $\sigma^2 = 4$ theilbar). Dann ist $(\sigma m, n, \sigma l)$, weil m relative Primzahl zu $2D$, eine ursprüngliche Form der σten Art von der Determinante D und folglich einer und nur einer in dem System S enthaltenen Form äquivalent*). Ist (a, b, c) diese Form des Systems, so liefert nur sie solche Darstellungen (x, y) der Zahl σm, welche zu der durch n repräsentirten Wurzel der obigen Congruenz gehören, und zwar ebenso viele verschiedene solche Darstellungen (x, y), als es Transformationen $\binom{x,\ \xi}{y,\ \eta}$ der Form (a, b, c) in die Form $(\sigma m, n, \sigma l)$, d. h. ebenso viele, als es Auflösungen (t, u) der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ giebt (§§. 60, 61, 62). Den Complex aller dieser

*) Da der Coefficient σm positiv ist, so gilt dies auch für den Fall, in welchem D negativ ist, und also S nur Formen mit positiven äusseren Coefficienten enthält.

Darstellungen der Zahl σm, welche zu einer und derselben durch n repräsentirten Wurzel der obigen Congruenz gehören, wollen wir eine *Gruppe* von Darstellungen nennen. Den 2^μ incongruenten Wurzeln dieser Congruenz entsprechen daher 2^μ solche Gruppen von Darstellungen derselben Zahl σm durch Formen des Systemes S, und in jeder Gruppe sind ebenso viel Darstellungen enthalten, als es Auflösungen der Gleichung $t^2 - Du^2 = \sigma^2$ giebt.

Das System der Zahlen m ist nun also vollständig definirt durch die Bedingungen:

1. *m ist positiv;*
2. *m ist relative Primzahl gegen* $2D$;
3. *D ist quadratischer Rest von m.*

§. 87.

Jetzt haben wir die Darstellungen von σm, welche einer und derselben Gruppe angehören genauer zu betrachten.

Für den Fall einer *negativen* Determinante D ist die Anzahl $\varkappa$ der Auflösungen (t, u) der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$ endlich; dieselbe ist zugleich die Anzahl aller zu einer Gruppe gehörenden Darstellungen einer jeden Zahl σm; bedeutet also μ wieder die Anzahl der verschiedenen in m aufgehenden Primzahlen f, so ist 2^μ die Anzahl der Gruppen, deren jede $\varkappa$ Darstellungen enthält, und folglich ist

$$\varkappa \,.\, 2^\mu$$

die Gesammtanzahl aller Darstellungen der Zahl σm; und hierin ist (§. 62)

$$\varkappa = 2 \text{ im Allgemeinen;}$$
$$\varkappa = 4, \text{ wenn } D = -1,$$
$$\varkappa = 6, \text{ wenn } D = -3 \text{ und } \sigma = 2$$

ist.

Für den Fall einer *positiven* Determinante D dagegen ist die Anzahl der Auflösungen (t, u) der unbestimmten Gleichung $t^2 - Du^2 = \sigma^2$, und folglich auch die Anzahl der in jeder der 2^μ Gruppen enthaltenen Darstellungen der Zahl σm *unendlich gross.* Wir gehen daher zunächst darauf aus, durch neue Bedingungen, welche den darstellenden Zahlen x, y aufzuerlegen sind, aus den

unendlich vielen in einer Gruppe enthaltenen Darstellungen stets *eine einzige* zu isoliren. Dazu betrachten wir die allgemeine Form aller derselben Gruppe angehörenden Darstellungen (x, y) der Zahl σm. Ist wieder (a, b, c) die Form des Systems S, mit welcher die Form $(\sigma m, n, \sigma l)$ äquivalent ist, und ist $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ eine bestimmte Transformation der erstern Form in die letztere, so erhält man (nach §. 61) aus dieser einen alle anderen durch die Zusammensetzung

$$\begin{pmatrix}\lambda, & \mu \\ \nu, & \varrho\end{pmatrix}\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}\lambda\alpha + \mu\gamma, & \lambda\beta + \mu\delta \\ \nu\alpha + \varrho\gamma, & \nu\beta + \varrho\delta\end{pmatrix}$$

aller Substitutionen $\binom{\lambda,\ \mu}{\nu,\ \varrho}$, durch welche (a, b, c) in sich selbst übergeht, mit dieser bestimmten Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$. Da nun (nach §. 60) jedesmal der erste und dritte Coefficient einer solchen Substitution eine zu der Wurzel n gehörende Darstellung liefern, und da auch umgekehrt jede solche Darstellung (x, y) auf diese Weise, und zwar nur ein einziges Mal erzeugt wird, so ist die allgemeine Form aller dieser Darstellungen folgende:

$$x = \lambda\alpha + \mu\gamma, \quad y = \nu\alpha + \varrho\gamma;$$

da (α, γ) selbst eine solche Darstellung ist, so kann man sagen, dass diese beiden Gleichungen aus einer bestimmten Darstellung (α, γ) alle derselben Gruppe angehörenden Darstellungen (x, y) finden lehren. Nun war aber (§. 62)

$$\lambda = \frac{t - bu}{\sigma}, \quad \mu = -\frac{cu}{\sigma},$$

$$\nu = \frac{au}{\sigma}, \quad \varrho = \frac{t + bu}{\sigma},$$

wo (t, u) jede beliebige Auflösung der Gleichung $t^2 - Du^2 = \sigma^2$ bedeutete; folglich erhalten wir

$$x = \alpha\frac{t}{\sigma} - (b\alpha + c\gamma)\frac{u}{\sigma}, \quad y = \gamma\frac{t}{\sigma} + (a\alpha + b\gamma)\frac{u}{\sigma}.$$

Für alle diese Werthe ist daher

$$ax^2 + 2bxy + cy^2 = \sigma m;$$

durch Multiplication mit dem ersten Coefficienten ergiebt sich wie früher

$$\sigma am = (ax + (b + \sqrt{D})y)\,(ax + (b - \sqrt{D})y),$$

und es tritt nun die höchst merkwürdige Erscheinung auf, dass jeder der beiden irrationalen Factoren rechter Hand eine geome-

trische Reihe constituirt; setzt man nämlich die vorstehenden Werthe von x, y ein, so ergiebt sich leicht

$$ax + (b + \sqrt{D})y = (a\alpha + (b + \sqrt{D})\gamma)\frac{t + u\sqrt{D}}{\sigma},$$

$$ax + (b - \sqrt{D})y = (a\alpha + (b - \sqrt{D})\gamma)\frac{t - u\sqrt{D}}{\sigma};$$

wenn man also mit T, U wie früher die kleinsten positiven Werthe von t, u bezeichnet und zur Abkürzung den positiven unechten Bruch

$$\frac{T + U\sqrt{D}}{\sigma} = \theta$$

setzt, so ist (nach §. 85)

$$ax + (b + \sqrt{D})y = \pm(a\alpha + (b + \sqrt{D})\gamma)\theta^n$$
$$ax + (b - \sqrt{D})y = \pm(a\alpha + (b - \sqrt{D})\gamma)\theta^{-n}$$

wo n eine beliebige positive oder negative ganze Zahl oder Null sein kann. Wir betrachten nur die erste dieser beiden Gleichungen, da aus ihr die zweite schon von selbst folgt. Ist nun k irgend ein von Null verschiedener reeller Zahlwerth, so leuchtet ein, dass man das Vorzeichen der rechten Seite und den Exponenten n stets und nur auf eine einzige Weise so bestimmen kann, dass der algebraische Werth von $ax + (b + \sqrt{D})y$ zwischen den Grenzen k und $k\theta$ liegt; denn nachdem das Zeichen $\pm$ so gewählt ist, dass $\pm(a\alpha + (b + \sqrt{D})\gamma)$ gleichstimmig mit k wird, giebt es nur noch ein einziges Glied der geometrischen Reihe zwischen den beiden vorgeschriebenen Grenzen, wenn man, um für jeden Fall Unbestimmtheit zu vermeiden, die eine derselben, z. B. $k\theta$, von dem Intervall ausschliesst. Durch diese Forderung für den Werth von $ax + (b + \sqrt{D})y$ ist dann aus der unendlichen Anzahl von Darstellungen (x, y) eine einzige vollständig isolirt. Es kommt jetzt nur noch darauf an, k zweckmässig zu wählen.

Dazu können wir immer voraussetzen, dass die, eine ganze Classe repräsentirende, Form (a, b, c) des Systems S einen *positiven* ersten Coefficienten a hat; denn es giebt ja in jeder Classe sogar reducirte Formen, welche diese Eigenschaft haben. Wir machen daher von jetzt ab diese Voraussetzung über die Wahl der in S enthaltenen Formen (für negative Determinanten haben wir schon früher dieselbe Forderung gemacht, um dort die eine Hälfte aller Classen ganz von der Betrachtung auszuschliessen)

und müssen sie dann natürlich für alles Folgende festhalten. Dann wählen wir für k die *positive* Quadratwurzel aus $\sigma a m$, was gestattet ist, da wir nur die positiven darstellbaren Zahlen σm betrachten. Wir stellen also die Bedingungen

$$\sqrt{\sigma a m} \leqq ax + (b + \sqrt{D})y < \theta\sqrt{\sigma a m}$$

auf, um aus allen derselben Gruppe angehörigen Darstellungen von σm durch (a, b, c) eine einzige (x, y) zu isoliren. Sie lassen sich, da ihre drei Glieder positiv sind, so umformen: quadrirt man, und bedenkt, dass $\sigma a m$ das Product aus zwei positiven irrationalen Factoren ist, so erhält man leicht durch Division

$$ax + (b - \sqrt{D})y \leqq ax + (b + \sqrt{D})y < \theta^2(ax + (b - \sqrt{D})y);$$

durch Vergleichung der beiden ersten Glieder ergiebt sich, da $\sqrt{D}$ stets *positiv* genommen wird, die Bedingung

$$y \geqq 0;$$

die beiden letzten Glieder geben durch Umstellung und Restitution des Werthes von θ die Bedingung

$$ax + by > \frac{T}{U}y.$$

Umgekehrt überzeugt man sich leicht, dass aus diesen beiden Bedingungen

$$y \geqq 0, \quad ax + by > \frac{T}{U}y$$

rückwärts die obigen ursprünglichen Isolirungsbedingungen folgen.

Ausserdem zeigt sich, was besonders zu bemerken ist, dass in Folge dieser beiden Bedingungen auch der Werth der Form $ax^2 + 2bxy + cy^2$ von selbst positiv ausfällt; denn da $T > U\sqrt{D}$ ist, so ergiebt sich durch Addition von $\pm y\sqrt{D}$ auf beiden Seiten der zweiten Bedingung, dass die beiden Factoren

$$ax + (b + \sqrt{D})y, \quad ax + (b - \sqrt{D})y$$

positiv sind, woraus dasselbe für ihr Product und also, da a positiv ist, auch für $ax^2 + 2bxy + cy^2$ folgt (für Formen von negativer Determinante versteht sich dies von selbst, da wir nur solche betrachten, deren äussere Coefficienten positiv sind).

§. 88.

Mit Rücksicht auf diese letzte Bemerkung können wir nun das Vorhergehende in folgender Weise noch einmal zusammenfassen:

Es sei S ein vollständiges System ursprünglicher Formen

$$(a, b, c), \quad (a', b', c') \ldots$$

der σten Art für eine gegebene Determinante D, mit positiven ersten Coefficienten a, a' . . . Dann setze man in jede dieser Formen, z. B. (a, b, c), für die Variabeln alle ganzzahligen Werthenpaare x, y ein, welche folgenden Bedingungen genügen:

I. $\dfrac{ax^2 + 2bxy + cy^2}{\sigma}$ *ist relative Primzahl zu 2D;*

II. *im Fall einer positiven Determinante D ist*

$$y \geqq 0, \quad ax + by > \frac{T}{U} y$$

wo T, U die kleinsten positiven der Gleichung

$$T^2 - DU^2 = \sigma^2$$

genügenden ganzen Zahlen bedeuten;

III. *x und y sind relative Primzahlen zu einander.*

Auf diese Weise werden durch die Formen S alle ganzen Zahlen σm und nur solche dargestellt, welche folgenden Bedingungen genügen:

1. *m ist positiv,*
2. *m ist relative Primzahl zu 2D,*
3. *D ist quadratischer Rest von m,*

und die Gesammtanzahl dieser Darstellungen einer jeden solchen Zahl σm ist gleich

$$\varkappa \,.\, 2^{\mu},$$

wo μ die Anzahl der in m aufgehenden verschiedenen Primzahlen bedeutet, während ϰ von m unabhängig ist, nämlich

$\varkappa = 1$ *für positive Determinanten D,*
$= 4$ *für* $D = -1$,
$= 6$ *für* $D = -3$ *und* $\sigma = 2$,
$= 2$ *in den übrigen Fällen.*

Dasselbe System der unendlich vielen Zahlen m kann daher auf doppelte Art erzeugt werden, erstens durch Zusammensetzung aus den Primzahlen f, von welchen D quadratischer Rest ist, und zweitens durch die Substitution aller erlaubten Zahlenpaare x, y in die Formen des Systems S. Dieses Resultat der früheren Untersuchungen über die Aequivalenz der Formen und die Darstellbarkeit der Zahlen bildet das *Grundprincip* der folgenden Untersuchung. Wir bemerken zunächst, dass die Identität der auf die beiden verschiedenen Arten erzeugten Zahlensysteme nicht aufhören wird, wenn wir von jeder der erzeugten Zahlen eine bestimmte Function ψ nehmen, d. h. es wird wieder Identität bestehen zwischen dem Complex der Zahlen

$$\psi\left(\frac{ax^2 + 2bxy + cy^2}{\sigma}\right), \quad \psi\left(\frac{a'x^2 + 2b'xy + c'y^2}{\sigma}\right) \ldots$$

und dem System der Zahlen $\psi(m)$, vorausgesetzt, dass der einem bestimmten Individuum m entsprechende Functionswerth $\psi(m)$ genau $\varkappa \,.\, 2^\mu$ mal in den letztern Complex aufgenommen wird. Ist daher die sonst ganz beliebige Function ψ so gewählt, dass die *Summe* aller dieser Werthe eine von der Anordnung derselben unabhängige convergente Reihe bildet, so folgt aus der angegebenen Identität die *Fundamentalgleichung*

$$\Sigma\, \psi\left(\frac{ax^2 + 2bxy + cy^2}{\sigma}\right) + \Sigma\, \psi\left(\frac{a'x^2 + 2b'xy + c'y^2}{\sigma}\right) + \cdots$$
$$= \varkappa\, \Sigma\, 2^\mu\, \psi(m).$$

Die linke Seite derselben besteht aus ebensoviel Hauptsummen, als das System S Formen (a, b, c), (a', b', c') . . . enthält, d. h. als es Formenclassen für diese Determinante giebt. Jede Hauptsumme, wie z. B.

$$\Sigma\, \psi\left(\frac{ax^2 + 2bxy + cy^2}{\sigma}\right)$$

ist eine doppelt unendliche Reihe, deren Glieder den sämmtlichen durch die Bedingungen I., II., III. definirten Zahlenpaaren x, y entsprechen (die Bedingungen I. und II. sind natürlich für die folgende Hauptsumme so zu modificiren, dass (a', b', c') an die Stelle von (a, b, c) tritt). Endlich bezieht sich die rechts angedeutete Summation auf alle aus den Primzahlen f zusammengesetzten Zahlen m, und ebenso behalten μ und $\varkappa$ ihre frühere Bedeutung. Wir specialisiren nun die Function ψ so, dass wir

$$\psi(z) = \frac{1}{z^s}$$

setzen, wo s ein beliebiger positiver Werth, aber > 1 ist; diese letztere Bedingung ist, wie wir später nachträglich zeigen werden, nothwendig, damit die vorstehenden unendlichen Reihen convergiren. Hierdurch geht unsere obige Gleichung in die folgende über:

$$\Sigma \left(\frac{ax^2 + 2bxy + cy^2}{\sigma}\right)^{-s} + \cdots = \varkappa \, \Sigma \frac{2^\mu}{m^s},$$

wo der Bequemlichkeit halber links nur eine einzige der den verschiedenen Formen entsprechenden Hauptsummen aufgeschrieben ist.

§. 89.

Wir beschäftigen uns nun zunächst mit einer Umformung *) der rechten Seite dieser Gleichung; zu dem Zweck betrachten wir das System

$$f_1, f_2, f_3 \ldots$$

der sämmtlichen Primzahlen f, welche nicht in $2D$ aufgehen, und von welchen D quadratischer Rest ist. Jede der oben definirten Zahlen m ist dann von der Form

$$f_1^{n_1} f_2^{n_2} f_3^{n_3} \ldots,$$

wo die Exponenten $n_1, n_2, n_3 \ldots$ positive ganze Zahlen oder Null sind, und jedes m kann auch nur auf eine einzige Weise in diese Form gebracht werden. Bilden wir nun die diesen Primzahlen entsprechenden unendlichen Reihen

$$1 + \frac{2}{f_1^s} + \frac{2}{f_1^{2s}} + \frac{2}{f_1^{3s}} + \cdots + \frac{2}{f_1^{n_1 s}} + \cdots$$

$$1 + \frac{2}{f_2^s} + \frac{2}{f_2^{2s}} + \frac{2}{f_2^{3s}} + \cdots + \frac{2}{f_2^{n_2 s}} + \cdots$$

$$1 + \frac{2}{f_3^s} + \frac{2}{f_3^{2s}} + \frac{2}{f_3^{3s}} + \cdots + \frac{2}{f_3^{n_3 s}} + \cdots \text{ u. s. w.,}$$

*) Wir machen darauf aufmerksam, dass diese Umformung auch auf die allgemeinere Reihe $\Sigma\, 2^\mu \psi(m)$ anwendbar ist, wenn nur die Function ψ für ganze Argumente der Bedingung $\psi(z)\,\psi(z') = \psi(zz')$ genügt (vergl. §. 124).

so erkennt man leicht mit Berücksichtigung der eben gemachten Bemerkung, dass das Product aller dieser Reihen nichts Anderes als die Summe

$$\Sigma \frac{2^\mu}{m^s}$$

ist. Denn das Product aus beliebigen Gliedern der ersten, zweiten, dritten Reihe u. s. f. hat die Form

$$\frac{2^\mu}{(f_1^{n_1} f_2^{n_2} f_3^{n_3} \ldots)^s} = \frac{2^\mu}{m^s},$$

wo μ die Anzahl der wirklich in m aufgehenden Primzahlen f bedeutet, d. h. derjenigen, deren Exponent n von Null verschieden ist; es entsteht daher auf diese Weise wirklich jedes Glied der genannten Reihe, und jedes auch nur ein einziges Mal. Da nun andererseits

$$1 + \frac{2}{f^s} + \frac{2}{f^{2s}} + \frac{2}{f^{3s}} + \cdots + \frac{2}{f^{ns}} + \cdots$$

$$= 1 + \frac{2}{f^s} \cdot \frac{1}{1 - \frac{1}{f^s}} = \frac{1 + \frac{1}{f^s}}{1 - \frac{1}{f^s}}$$

ist, so erhalten wir folgende Gleichung

$$\Sigma \frac{2^\mu}{m^s} = \Pi \frac{1 + \frac{1}{f^s}}{1 - \frac{1}{f^s}},$$

in welcher das Productzeichen Π sich auf die sämmtlichen oben definirten Primzahlen f bezieht.

Bezeichnen wir mit q allgemein *jede positive nicht in* $2\,D$ *aufgehende Primzahl*, so leuchtet ein, dass man die vorstehende Gleichung auch in folgender Form schreiben kann:

$$\Sigma \frac{2^\mu}{m^s} = \Pi \frac{1 + \frac{1}{q^s}}{1 - \left(\frac{D}{q}\right) \frac{1}{q^s}};$$

denn so oft q nicht zu den Primzahlen f gehört, reducirt sich der entsprechende Factor des Productes auf $+ 1$. In der so erhaltenen

Gleichung multipliciren wir Zähler und Nenner des allgemeinen Factors zur Rechten mit $1 - q^{-s}$, wodurch derselbe gleich

$$\frac{1-\frac{1}{q^{2s}}}{\left(1-\frac{1}{q^s}\right)\left(1-\left(\frac{D}{q}\right)\frac{1}{q^s}\right)} = \frac{\left(\frac{1}{1-\frac{1}{q^s}}\right)\cdot\left(\frac{1}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}}\right)}{\left(\frac{1}{1-\frac{1}{q^{2s}}}\right)}$$

wird, und indem wir das unendliche Product in drei unendliche Producte zerlegen, erhalten wir

$$\Sigma \frac{2\mu}{m^s} = \frac{\Pi \frac{1}{1-\frac{1}{q^s}} \cdot \Pi \frac{1}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}}}{\Pi \frac{1}{1-\frac{1}{q^{2s}}}}.$$

Jetzt können wir endlich jedes der drei rechts befindlichen Producte wieder in eine unendliche Reihe verwandeln. Da nämlich

$$\frac{1}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}} = \Sigma \left(\frac{D}{q}\right)^r \frac{1}{q^{rs}} =$$

$$1 + \left(\frac{D}{q}\right)\frac{1}{q^s} + \left(\frac{D}{q}\right)^2 \frac{1}{q^{2s}} + \cdots + \left(\frac{D}{q}\right)^r \frac{1}{q^{rs}} + \cdots$$

ist, so wird, wenn man für q alle, nicht in $2D$ aufgehenden, Primzahlen

$$q_1, q_2, q_3 \ldots$$

setzt, das Product aller dieser Factoren gleich der Summe aller Glieder von der Form

$$\left(\frac{D}{q_1}\right)^{r_1}\left(\frac{D}{q_2}\right)^{r_2}\left(\frac{D}{q_3}\right)^{r_3}\cdots\frac{1}{(q_1^{r_1}\, q_2^{r_2}\, q_3^{r_3}\ldots)^s},$$

wo die Exponenten $r_1, r_2, r_3 \ldots$ alle positiven ganzen Zahlen und Null zu durchlaufen haben. Das System aller der in den Nennern unter dem Exponenten s vorkommenden Zahlen

$$q_1^{r_1}\, q_2^{r_2}\, q_3^{r_3} \ldots = n$$

besteht offenbar aus sämmtlichen *positiven ganzen Zahlen n, welche relative Primzahlen gegen $2D$ sind*; jede solche Zahl n wird einmal und auch nur einmal durch ein bestimmtes System von Expo-

nenten $r_1, r_2, r_3 \ldots$ erzeugt; gleichzeitig ist dann mit Benutzung der von *Jacobi* erweiterten Bedeutung des Legendre'schen Zeichens

$$\left(\frac{D}{q_1}\right)^{r_1}\left(\frac{D}{q_2}\right)^{r_2}\left(\frac{D}{q_3}\right)^{r_3}\cdots = \left(\frac{D}{q_1{}^{r_1}}\right)\left(\frac{D}{q_2{}^{r_2}}\right)\left(\frac{D}{q_3{}^{r_3}}\right)\cdots$$
$$= \left(\frac{D}{q_1{}^{r_1}\, q_2{}^{r_2}\, q_3{}^{r_3}\ldots}\right) = \left(\frac{D}{n}\right).$$

Hierdurch gewinnen wir also folgende Verwandlung

$$\Pi \frac{1}{1-\left(\frac{D}{q}\right)\frac{1}{q^s}} = \Sigma\left(\frac{D}{n}\right)\frac{1}{n^s},$$

wo das Summenzeichen rechts sich auf alle positiven Zahlen n bezieht, die relative Primzahlen gegen $2\,D$ sind.

Verfährt man ganz ebenso, indem man alle die Entwickelungen

$$\frac{1}{1-\frac{1}{q^s}} = 1 + \frac{1}{q^s} + \frac{1}{q^{2s}} + \cdots + \frac{1}{q^{rs}} + \cdots$$

mit einander multiplicirt, so erhält man offenbar

$$\Pi \frac{1}{1-\frac{1}{q^s}} = \Sigma \frac{1}{n^s}$$

uud folglich auch

$$\Pi \frac{1}{1-\frac{1}{q^{2s}}} = \Sigma \frac{1}{n^{2s}}.$$

Hierdurch haben wir die wichtige Umformung

$$\Sigma \frac{2^\mu}{m^s} = \frac{\Sigma \frac{1}{n^s} \times \Sigma\left(\frac{D}{n}\right)\frac{1}{n^s}}{\Sigma \frac{1}{n^{2s}}}$$

gewonnen.

§. 90.

Wir multipliciren nun beide Seiten unserer Hauptgleichung (§. 88) mit der unendlichen Reihe

$$\Sigma \frac{1}{n^{2s}},$$

wodurch sie dem eben gewonnenen Resultat gemäss in die folgende übergeht:

$$\Sigma \frac{1}{n^{2s}} \times \Sigma \left(\frac{ax^2 + 2bxy + cy^2}{\sigma}\right)^{-s} + \cdots = \varkappa \Sigma \frac{1}{n^s} \times \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}.$$

Führen wir in dem ersten Gliede links die Multiplication der beiden Summen aus, so kann das Resultat als die dreifach unendliche Reihe

$$\Sigma \left(\frac{an^2x^2 + 2bn^2xy + cn^2y^2}{\sigma}\right)^{-s}$$

geschrieben werden, in welcher für x, y alle den früheren Bedingungen I., II., III. genügenden Werthe (§. 88), und für n alle positiven relativen Primzahlen gegen $2D$ zu setzen sind. Diese Reihe kann man aber auch wieder als eine doppelt unendliche ansehen, wenn man

$$nx = x', \quad ny = y'$$

setzt; denn dann nimmt sie die Gestalt

$$\Sigma \left(\frac{ax'^2 + 2bx'y' + cy'^2}{\sigma}\right)^{-s}$$

an, und es fragt sich nur, welche Bedingungen den neuen Summationsbuchstaben x', y' aufzuerlegen sind. Diese ergeben sich aus den Bedingungen für x, y, n folgendermassen. Erstens: Da x, y zufolge der Bedingung I. so gewählt werden müssen, dass

$$\frac{ax^2 + 2bxy + cy^2}{\sigma}$$

relative Primzahl gegen $2D$ wird, und da n ebenfalls relative Primzahl gegen $2D$ ist, so gilt dasselbe von

$$\frac{ax'^2 + 2bx'y' + cy'^2}{\sigma} = n^2 \cdot \frac{ax^2 + 2bxy + cy^2}{\sigma}.$$

Zweitens: für den Fall einer positiven Determinante waren x, y den Isolirungsbedingungen II.

$$y \geqq 0, \quad ax + by > \frac{T}{U} y$$

zu unterwerfen; multiplicirt man dieselben mit n, so ergeben sich die ganz gleichlautenden Bedingungen

$$y' \geqq 0, \quad ax' + by' > \frac{T}{U} y'.$$

Drittens: aus der Bedingung, dass x, y relative Primzahlen sein sollen, würde jetzt nur noch folgen, dass der grösste gemeinschaftliche Divisor n von x', y' relative Primzahl gegen $2D$ sein muss; allein diese Bedingung kann man gänzlich fallen lassen, da sie schon in der ersten enthalten ist; denn sobald x', y' einen gemeinschaftlichen Divisor hätten, der nicht relative Primzahl gegen $2D$ wäre, so könnte auch

$$\frac{ax'^2 + 2bx'y' + cy'^2}{\sigma}$$

nicht relative Primzahl gegen $2D$ sein.

Es zeigt sich also, dass die neuen Variabeln x', y' nur den beiden Bedingungen I. und II. zu unterwerfen sind, wenn man in denselben die Variabeln accentuirt, dass dagegen die Bedingung III. ganz fortgefallen ist. Umgekehrt überzeugt man sich leicht, dass ein jedes solches Werthenpaar x', y' einmal und nur einmal durch ein Werthenpaar x, y und eine Zahl n erzeugt wird.

Wir lassen nun der Bequemlichkeit halber die Accente der Variabeln wieder fort, und schreiben daher unsere Hauptgleichung in folgender Form *)

$$\Sigma \left(\frac{ax^2 + 2bxy + cy^2}{\sigma}\right)^{-s} + \cdots = \varkappa\, \Sigma \frac{1}{n^s} \times \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s},$$

wo nun in der ersten auf die Form (a, b, c) bezüglichen Hauptsumme die Summationsbuchstaben nur noch den beiden folgenden Bedingungen zu unterwerfen sind:

I. Der Werth $\frac{ax^2 + 2bxy + cy^2}{\sigma}$ soll relative Primzahl gegen $2D$ sein.

II. Im Fall einer positiven Determinante soll

$$y \geqq 0, \quad ax + by > \frac{T}{U} y$$

sein, wo T, U die frühere Bedeutung haben.

*) Auf dieselbe Weise kann auch die allgemeinere Gleichung abgeleitet werden, in welcher statt der Function z^{-s} irgend eine Function $\psi(z)$ auftritt, welche der Bedingung $\psi(z)\psi(z') = \psi(zz')$ genügt, so oft z und z' ganze Zahlen sind.

§. 91.

Bevor wir weitergehen, wollen wir aus unserer letzten Gleichung einige interessante Folgerungen ziehen: die erste derselben ist rein zahlentheoretischer Natur und vervollständigt unsere frühere Theorie der Darstellung. Wir multipliciren die beiden unendlichen Reihen

$$\Sigma \frac{1}{n'^s}, \quad \Sigma \left(\frac{D}{n''}\right) \frac{1}{n''^s}$$

rechter Hand, nachdem wir die Summationsbuchstaben, um sie von einander zu unterscheiden, accentuirt haben; dann erhalten wir als Product die doppelt unendliche Reihe

$$\Sigma \left(\frac{D}{n''}\right) \frac{1}{(n'n'')^s},$$

in welcher sowohl n' als auch n'' das Gebiet aller Zahlen n, d. h. aller derjenigen positiven ganzen Zahlen zu durchlaufen hat, welche relative Primzahlen gegen $2D$ sind. Offenbar ist jedes Product von der Form $n'n''$ wieder in demselben Gebiet enthalten; fassen wir daher alle Glieder der Doppelsumme, in welchen das Product $n'n''$ denselben Werth n hat, immer in ein einziges zusammen, so können wir diese Doppelsumme wieder in die Form einer einfach unendlichen Reihe

$$\Sigma \frac{\tau_n}{n^s}$$

bringen; bezeichnet man mit δ die sämmtlichen Divisoren der Zahl n, so wird offenbar

$$\tau_n = \Sigma \left(\frac{D}{\delta}\right).$$

Dividiren wir ferner die Gleichung auf beiden Seiten durch σ^s, so nimmt sie folgende Form an

$$\Sigma \frac{1}{(ax^2 + 2bxy + cy^2)^s} + \cdots = \Sigma \frac{\varkappa \tau_n}{(\sigma n)^s}.$$

Fassen wir nun auch links alle in den verschiedenen Doppelsummen vorkommenden Glieder, welche denselben Werth haben, in ein einziges zusammen, so erhalten wir folgende Gleichung

$$\Sigma \frac{\lambda_\nu}{\nu^s} = \Sigma \frac{\varkappa \tau_n}{(\sigma n)^s},$$

wo mit ν alle die durch die sämmtlichen Formen $(a, b, c) \ldots$ des Systems S darstellbaren Zahlen bezeichnet werden, und λ_ν die Anzahl der verschiedenen Darstellungen einer solchen Zahl ν bedeutet. Hierbei ist wohl zu bemerken, dass jetzt ebensowohl uneigentliche wie eigentliche Darstellungen zugelassen werden, indem die darstellenden Zahlen x, y nur noch den Bedingungen I. und II. des vorigen Paragraphen unterworfen sind, während sie früher auch relative Primzahlen unter einander sein mussten.

Besteht nun für jeden über einer gewissen Grenze liegenden positiven Werth des Exponenten s eine Gleichung von der Form

$$\frac{\alpha}{a^s} + \frac{\beta}{b^s} + \frac{\gamma}{c^s} + \cdots = \frac{\alpha'}{a'^s} + \frac{\beta'}{b'^s} + \frac{\gamma'}{c'^s} + \cdots$$

wo $a, b, c \ldots$ sowohl wie $a', b', c' \ldots$ positive und in ihrer Aufeinanderfolge wachsende Zahlwerthe bedeuten, und sind die sämmtlichen Coefficienten $\alpha, \beta, \gamma \ldots \alpha', \beta', \gamma' \ldots$ von Null verschieden, so folgt hieraus die vollständige Identität beider Reihen, d. h. es ist

$$a = a', \quad b = b', \quad c = c' \ldots$$
$$\alpha = \alpha', \quad \beta = \beta', \quad \gamma = \gamma' \ldots$$

Um dies zu beweisen, können wir annehmen, es sei $a \leqq a'$; multipliciren wir beide Seiten der Gleichung mit a^s, so erhalten wir

$$\alpha + \beta\left(\frac{a}{b}\right)^s + \gamma\left(\frac{a}{c}\right)^s + \cdots$$
$$= \alpha'\left(\frac{a}{a'}\right)^s + \beta'\left(\frac{a}{b'}\right)^s + \gamma'\left(\frac{a}{c'}\right)^s + \cdots$$

Da nun sowohl die Werthe

$$\frac{a}{b}, \frac{a}{c} \cdots$$

als auch die Werthe

$$\frac{a}{b'}, \frac{a}{c'} \cdots$$

fortwährend abnehmende echte Brüche sind, und beide Reihen convergiren, so überzeugt man sich leicht*), dass mit unbegrenzt wachsendem s die linke Seite der vorstehenden Gleichung sich dem Grenzwerth α nähert, und ebenso die rechte dem Grenzwerth α' oder 0, je nachdem $a = a'$ oder $< a'$ ist. Da nun beide Seiten

*) Vergl Supplement IX. §. 143.

sich nothwendig demselben Grenzwerth nähern müssen, und α von Null verschieden ist, so muss $a = a'$, und folglich auch $\alpha = \alpha'$ sein. Nachdem so die Identität der ersten Glieder auf beiden Seiten bewiesen ist, kann man dieselben fortlassen; aus der so entstehenden Gleichung

$$\frac{\beta}{b^s} + \frac{\gamma}{c^s} + \cdots = \frac{\beta'}{b'^s} + \frac{\gamma'}{c'^s} + \cdots$$

folgt dann auf dieselbe Weise, dass $b = b'$ und $\beta = \beta'$ sein muss, und so kann man fortfahren.

Wendet man dies Princip auf unsere obige Gleichung an, so ergiebt sich, dass jedes σn, dem ein von Null verschiedenes τ_n entspricht, nothwendig eine Zahl ν, d. h. eine durch die Formen S darstellbare Zahl, und dass die Anzahl λ_ν der verschiedenen Darstellungen eines solchen $\nu = \sigma n$ gleich $\varkappa \tau_n$ ist; wenn dagegen $\tau_n = 0$ ist, so kann auch σn keine durch die Formen S darstellbare Zahl ν sein; wir können daher in beiden Fällen sagen: *die Anzahl aller Darstellungen einer Zahl σn durch die Formen S ist immer*

$$= \varkappa \tau_n = \varkappa \sum \left(\frac{D}{\delta}\right),$$

wo δ alle Divisoren der Zahlen n durchlaufen muss).*

Wir wollen dieses Resultat auf einige Beispiele anwenden.

1. Ist $D = -1$ (und folglich $\sigma = 1$), so ist nur eine einzige Form in dem System S enthalten, für welche wir die Form $(1, 0, 1)$ wählen können; das System der Zahlen σn ist das der positiven ungeraden Zahlen, und da $\varkappa = 4$ ist, so erhalten wir das Resultat:

Die Anzahl aller Darstellungen einer beliebigen positiven ungeraden Zahl n durch die Form $(1, 0, 1) = x^2 + y^2$ ist gleich

$$4 \sum (-1)^{\frac{1}{2}(\delta-1)} = 4(M-N)$$

d. h. gleich dem vierfachen Ueberschuss der Anzahl M ihrer Divisoren δ von der Form $4h+1$ über die Anzahl N der Divisoren δ von der Form $4h+3$.

Die darstellenden Zahlen x, y sind gar keiner Beschränkung unterworfen; es leuchtet ferner ein, dass jedesmal acht verschiedene Darstellungen eine einzige Zerlegung in zwei Quadrate geben; nur wenn eine der beiden darstellenden Zahlen $= 0$ ist, findet eine

*) Vergl. §. 124.

Ausnahme Statt, weil dann nur vier verschiedene Darstellungen dieselbe Zerlegung liefern, ein Fall, der nur dann eintreten kann, wenn n eine Quadratzahl ist. Die Anzahl der verschiedenen Zerlegungen ist daher $\frac{1}{2}(M - N + 1)$ oder $\frac{1}{2}(M - N)$, je nachdem n eine Quadratzahl ist oder nicht. So ist z. B.

$$25 = 0^2 + 5^2 = 3^2 + 4^2$$
$$45 = 3^2 + 6^2$$
$$49 = 0^2 + 7^2$$
$$65 = 1^2 + 8^2 = 4^2 + 7^2.$$

Ist endlich n eine Primzahl, so ergiebt sich wieder, dass n auf eine einzige, oder auf gar keine Weise in zwei Quadrate zerlegt werden kann, je nachdem n von der Form $4h + 1$, oder von der Form $4h + 3$ ist (§. 68).

2. Für die positive Determinante $D = 2$ existiren nur die beiden einander äquivalenten reducirten Formen $(1, 1, -1)$ und $(-1, 1, 1)$, also nur eine einzige Classe; als repräsentirende Form kann man daher auch $(1, 0, -2) = x^2 - 2y^2$ wählen. Da die kleinsten der Gleichung $t^2 - 2u^2 = 1$ genügenden Zahlen $T = 3$, $U = 2$ sind, so werden nur solche Darstellungen betrachtet, in welchen $y \geqq 0$, $2x > 3y$ ist. Da ferner

$$\left(\frac{2}{\delta}\right) = (-1)^{\frac{1}{8}(\delta^2 - 1)} = +1 \text{ oder } = -1$$

ist, je nachdem $\delta = 8h \pm 1$ oder $\delta = 8h \pm 5$ ist, so bekommen wir folgendes Resultat:

Die Anzahl aller den obigen Bedingungen genügenden Darstellungen (x, y) einer beliebigen positiven ungeraden Zahl n durch die Form $x^2 - 2y^2$ ist gleich dem Ueberschuss der Anzahl der Divisoren von n, welche die Form $8h \pm 1$ haben, über die Anzahl der anderen Divisoren.

§. 92.

Eine zweite interessante Anwendung der vorstehenden Untersuchung machen wir auf die Analysis. Wir haben gesehen, dass durch Einsetzen aller den Bedingungen I. und II. genügenden ganzzahligen Werthenpaare x, y in die Formen $(a, b, c)\ldots$ des Systems S die Zahlen σn erzeugt werden, und zwar ist

$$\varkappa\tau_n = \varkappa \sum \left(\frac{D}{\delta}\right)$$

die Anzahl der verschiedenen Erzeugungen einer solchen Zahl σn, wenn wieder für δ alle Divisoren von n gesetzt werden. Nehmen wir daher von jeder der Zahlen $ax^2 + 2bxy + cy^2$ eine bestimmte Function ψ, so entsteht auf diese Weise jeder Werth $\psi(\sigma n)$ so oft als $\varkappa\tau_n$ angiebt. Hieraus folgt wieder, dass

$$\sum \psi(ax^2 + 2bxy + cy^2) + \cdots = \varkappa \sum \tau_n \psi(\sigma n)$$

sein wird, sobald die Function ψ so gewählt wird, dass diese unendlichen Reihen bestimmte von der Anordnung ihrer Glieder unabhängige Summen haben. Dies ist der Fall, wenn man

$$\psi(z) = q^z$$

setzt, wo q eine reelle oder complexe Grösse bedeutet, deren Modulus ein echter Bruch ist. Man erhält auf diese Weise folgende sehr allgemeine Gleichung

$$\sum q^{ax^2+2bxy+cy^2} + \cdots = \varkappa \sum \tau_n q^{\sigma n};$$

da auf der rechten Seite der Coefficient τ_n selbst wieder eine Summe ist, in welcher δ die sämmtlichen Divisoren von n zu durchlaufen hat, so kann man, indem man n in $n'\delta$ verwandelt, die Gleichung auch so schreiben

$$\sum q^{ax^2+2bxy+cy^2} + \cdots = \varkappa \sum \left(\frac{D}{\delta}\right) q^{\sigma n'\delta},$$

wo nun rechts eine Doppelsumme steht, in welcher jeder der beiden Summationsbuchstaben n' und δ das Gebiet aller Zahlen n zu durchlaufen hat.

Wir wollen die vorstehende Gleichung auf einige specielle Fälle anwenden. Nehmen wir z. B. $D = -1$, also $\sigma = 1$, so haben wir links nur eine einzige Doppelsumme; nehmen wir wieder (1, 0, 1) als die repräsentirende Form, so ist dieselbe gleich

$$\sum q^{x^2+y^2},$$

worin x, y alle Werthenpaare zu durchlaufen haben, für welche $x^2 + y^2$ ungerade ausfällt; es muss daher eine der beiden Zahlen x, y ungerade, die andere gerade sein; da man nun in jeder erlaubten Combination x mit y vertauschen kann, so setzen wir fest, dass x nur die ungeraden, y nur die geraden Werthe durchlaufen soll, müssen dann aber die so beschränkte Doppelreihe mit 2 multipliciren; wir erhalten so

$$2 \sum q^{x^2+y^2} = 2 \sum q^{x^2} q^{y^2} = 2 \sum q^{x^2} \times \sum q^{y^2}$$

wo x alle positiven und negativen ungeraden, y alle positiven und negativen geraden Zahlen und Null zu durchlaufen hat; beschränken wir aber x auf alle positiven ungeraden, und y auf alle positiven geraden Zahlen, so können wir das vorstehende Product auch so schreiben

$$4 \sum q^{x^2} \times (1 + 2 \sum q^{y^2}).$$

Auf der rechten Seite haben wir (nach §. 88) die Doppelsumme

$$4 \sum \left(\frac{-1}{\delta}\right) q^{n'\delta} = 4 \sum (-1)^{\frac{1}{2}(\delta-1)} q^{n'\delta},$$

wo n' und δ alle positiven ungeraden Zahlen zu durchlaufen haben; die Summation in Bezug auf n' lässt sich ausführen, indem

$$\sum q^{n'\delta} = q^{\delta} + q^{3\delta} + q^{5\delta} + \cdots = \frac{q^{\delta}}{1 - q^{2\delta}}$$

ist; dadurch wird die rechte Seite gleich

$$4 \sum (-1)^{\frac{1}{2}(\delta-1)} \frac{q^{\delta}}{1 - q^{2\delta}}$$

und wir erhalten daher folgende merkwürdige Gleichung

$$(q + q^9 + q^{25} + q^{49} + \cdots)(1 + 2q^4 + 2q^{16} + 2q^{36} + \cdots)$$
$$= \frac{q}{1-q^2} - \frac{q^3}{1-q^6} + \frac{q^5}{1-q^{10}} - \frac{q^7}{1-q^{14}} + \cdots$$

welche, wie die anderen Gleichungen, welche negativen Determinanten entsprechen, auch aus der Theorie der *Elliptischen Functionen* abgeleitet werden kann*).

Für positive Determinanten fallen die entsprechenden Gleichungen weniger einfach aus, weil auf der linken Seite die Variabeln x, y immer noch der Bedingung II. unterworfen sind. Nehmen wir z. B. $D = 2$, also $\sigma = 1$, $\varkappa = 1$, so erhalten wir in ähnlicher Weise die Gleichung

$$\sum q^{x^2-2y^2} = \sum \left(\frac{2}{\delta}\right) q^{\delta n'}$$
$$= \frac{q}{1-q^2} - \frac{q^3}{1-q^6} - \frac{q^5}{1-q^{10}} + \frac{q^7}{1-q^{14}} + \cdots,$$

wo auf der linken Seite für x, y alle Werthenpaare zu setzen sind,

---

*) Man vergleiche *Jacobi: Fundamenta nova theoriae functionum ellipticarum* 1829 pagg. 92, 103, 184.

die den Bedingungen $y \geqq 0$, $2x > 3y$ genügen, und für welche ausserdem $x^2 - 2y^2$ und also x ungerade ist.

§. 93.

Wir kehren nun zu unserem eigentlichen Gegenstande, der weitern Behandlung der Gleichung (§. 90)

$$\Sigma \left(\frac{ax^2 + 2bxy + cy^2}{\sigma}\right)^{-s} + \cdots = \varkappa \, \Sigma \frac{1}{n^s} \times \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

zurück, und es wird gut sein, den Gang der Untersuchung hier mit wenigen Worten im Voraus anzugeben. Man würde auf unübersteigliche Schwierigkeiten stossen, wenn man die auf der linken Seite angedeuteten Summationen für einen beliebigen Werth von $s > 1$ wirklich ausführen wollte. Lässt man dagegen den Exponenten s immer mehr abnehmen und gegen den Werth 1 convergiren, so wird gleichzeitig jede dieser Hauptsummen über alle Grenzen wachsen, und bei näherer Betrachtung zeigt sich, dass das Product aus einer solchen Hauptsumme und aus $(s-1)$ sich einem festen endlichen Grenzwerth L nähert, welcher nur von der allen Formen gemeinschaftlichen Determinante D abhängt, und folglich wird der Grenzwerth der ganzen mit $(s-1)$ multiplicirten linken Seite $= hL$ sein, wenn man mit h die Anzahl der Hauptsummen, d. h. also die Anzahl der in dem Formensystem S enthaltenen Formen $(a, b, c) \ldots$ bezeichnet. Da ferner der Grenzwerth der mit $(s-1)$ multiplicirten rechten Seite sich direct bestimmen lässt, so erhält man auf diese Weise einen Ausdruck für die Classenanzahl h, deren Bestimmung ja den Gegenstand unserer ganzen Untersuchung bildet.

Bevor wir aber dazu übergehen, diesen Grenzprocess durchzuführen, müssen wir noch einige vorläufige Fragen erörtern, deren Beantwortung für unsern Zweck durchaus erforderlich ist. Zunächst wenden wir uns dazu, die den Summationsbuchstaben x, y auferlegte Bedingung I. (§. 90) so umzuformen, dass man einen deutlichen Ueberblick über das System der ihr genügenden Werthenpaare x, y erhält. Zu dem Ende dürfen wir annehmen, dass der Repräsentant (a, b, c) einer ganzen Classe immer so gewählt ist, dass der Quotient $a : \sigma$ nicht nur, wie schon früher festgesetzt

wurde, positiv, sondern auch *relative Primzahl gegen* $2D$ ist. Von der Berechtigung zu dieser Annahme wird man sich durch die folgende Betrachtung überzeugen. Ist

$$(a, b, c) = \sigma(Ax^2 + Bxy + Cy^2) = \sigma F$$

eine beliebige Form vom Theiler σ, und r irgend eine Primzahl, so kann man den beiden Variabeln x, y der Form stets solche Werthe beilegen, dass der Werth von F nicht durch r theilbar wird; denn ist eine der beiden Zahlen A, C, z. B. A, nicht durch r theilbar, so gebe man x einen durch r nicht theilbaren, y dagegen einen durch r theilbaren Werth; sind aber beide Coefficienten A, C durch r theilbar, so ist B gewiss nicht durch r theilbar, und folglich genügt es dann, x und y Werthe beizulegen, die beide nicht durch r theilbar sind. *Man kann folglich auch x und y immer so wählen, dass der Werth von F relative Primzahl gegen irgend eine vorgeschriebene Zahl k wird;* denn bezeichnet man mit r', r'', r''' ... die sämmtlichen in k aufgehenden Primzahlen, so braucht man nur zu bewirken, dass F durch keine einzige derselben theilbar wird, was nach dem eben Gesagten sich stets dadurch erreichen lässt, dass die beiden Variabeln x, y durch einige dieser Primzahlen theilbar, durch andere nicht theilbar angenommen werden — Bedingungen, die sich stets auf unendlich viele verschiedene Arten erfüllen lassen. Man kann hinzufügen, dass x, y ausserdem noch so gewählt werden können, dass der Werth von F *positiv* ausfällt; für eine negative Determinante D versteht sich dies von selbst, da wir Formen mit negativen äusseren Coefficienten ausschliessen; für eine positive Determinante braucht man, da

$$a\sigma F = (ax + by)^2 - Dy^2$$

ist, nur dafür zu sorgen, dass, je nachdem a positiv oder negativ ist, entsprechend $(ax + by)$ absolut genommen grösser oder kleiner als $y\sqrt{D}$ ausfällt, und offenbar lassen die bisher den Variabeln x, y auferlegten Bedingungen, durch einige Primzahlen theilbar, durch einige andere nicht theilbar zu sein, noch solchen Spielraum für ihr Grössenverhältniss, dass auch dieser Forderung noch auf unendlich viele verschiedene Arten genügt werden kann. Endlich können wir noch behaupten, dass für die Variabeln x, y auch solche Werthe gewählt werden können, welche unter einander *relative Primzahlen* sind und doch die übrigen Bedingungen erfüllen, dass F positiv und relative Primzahl gegen die vorgeschriebene Zahl k ist; denn haben x und y einen gemeinschaftlichen Divisor, so braucht

man sie nur durch Division von demselben zu befreien, und die Quotienten, die unter einander relative Primzahlen sind, bilden ein solches allen Anforderungen genügendes Werthenpaar.

Wir machen von der vorstehenden (auch für andere Untersuchungen nützlichen) Betrachtung eine specielle Anwendung auf den Fall, in welchem $k = 2D$ ist; wir können dann so sagen: ist (a, b, c) irgend eine Form vom Theiler σ und von der Determinante D, so kann man stets zwei relative Primzahlen α, γ von der Beschaffenheit finden, dass

$$\frac{a'}{\sigma} = \frac{a\alpha^2 + 2b\alpha\gamma + c\gamma^2}{\sigma}$$

positiv und relative Primzahl gegen $2D$ wird. Da nun α, γ relative Primzahlen sind, so kann man (§. 24) irgend ein Paar von Werthen β, δ wählen, welche der Gleichung $\alpha\delta - \beta\gamma = 1$ genügen, und dann geht die Form (a, b, c) durch die Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ in eine äquivalente Form über, deren erster Coefficient a' positiv ist und ausserdem die Eigenschaft hat, dass $a' : \sigma$ relative Primzahl gegen $2D$ ist. Und hiermit ist in der That der verlangte Nachweis geliefert, dass in jeder Formenclasse solche Repräsentanten ausgewählt werden können, welche die obige neue Bedingung erfüllen.

§. 94.

Wir nehmen daher jetzt an, dass die repräsentirende Form (a, b, c) so gewählt ist, dass $a : \sigma$ nicht nur positiv, sondern auch relative Primzahl gegen $2D$ ist, und fragen nun nach dem System aller Werthenpaare x, y, welche der Bedingung I. genügen, dass

$$\frac{ax^2 + 2bxy + cy^2}{\sigma}$$

relative Primzahl gegen $2D$ wird*). Bezeichnen wir wie früher mit $\varDelta$ den absoluten Werth der Determinante D, so kann man stets

$$x = 2\varDelta v + \alpha, \quad y = 2\varDelta w + \gamma$$

setzen, wo α und γ irgend welche der $2\varDelta$ Zahlen

$$0, 1, 2, \ldots (2\varDelta - 1),$$

---

*) Ganz ähnlich lässt sich auch der Fall behandeln, wenn (a, b, c) keine *ursprüngliche* Form ist; man kann dann gleich darauf ausgehen, die Anzahl der Classen von *beliebigem* Theiler σ zu bestimmen, und erhält auf diese Weise ebenfalls das unten (in §. 100) gewonnene Resultat.

und v und w beliebige ganze reelle Zahlen bedeuten; jede Combination zweier ganzen Zahlen x, y kann stets nur auf eine einzige Weise in diese Form gebracht werden. Da nun aus

$$x \equiv \alpha \text{ (mod. } 2\Delta) \quad \text{und} \quad y \equiv \gamma \text{ (mod. } 2\Delta)$$

auch

$$\frac{ax^2 + 2bxy + cy^2}{\sigma} \equiv \frac{a\alpha^2 + 2b\alpha\gamma + c\gamma^2}{\sigma} \text{ (mod. } 2\Delta)$$

folgt, so leuchtet ein, dass man unter den sämmtlichen $4\Delta^2$ Combinationen (α, γ) nur diejenigen zu ermitteln hat, für welche

$$\frac{a\alpha^2 + 2b\alpha\gamma + c\gamma^2}{\sigma}$$

relative Primzahl gegen 2Δ wird. Die gesuchten Combinationen (x, y) vertheilen sich dann in zusammengehörige Paare von arithmetischen Reihen, deren Differenz $= 2\Delta$ ist, und deren Anfangsglieder α, γ specielle solche Combinationen sind, die dieselbe Bedingung erfüllen. Uns kommt es nun weniger darauf an, wirklich alle diese Combinationen (α, γ) genau zu definiren, als vielmehr, nur ihre *Anzahl* sicher festzustellen, weil diese allein bei dem spätern Grenzübergang eine Rolle spielt. Hierzu ist es aber nöthig verschiedene Fälle zu unterscheiden.

Erstens: $\sigma = 1$. Wir fragen nach der Anzahl der Combinationen (α, γ), für welche $a\alpha^2 + 2b\alpha\gamma + c\gamma^2$ oder, da a relative Primzahl gegen 2Δ ist, für welche

$$a(a\alpha^2 + 2b\alpha\gamma + c\gamma^2) = (a\alpha + b\gamma)^2 \pm \Delta\gamma^2$$

relative Primzahl gegen 2Δ wird. Setzt man zunächst für γ irgend eine der Δ geraden Zahlen

$$0, 2, 4 \ldots (2\Delta - 2),$$

so ist erforderlich und hinreichend, dass $(a\alpha + b\gamma)^2$ und folglich $(a\alpha + b\gamma)$ relative Primzahl gegen 2Δ werde; lässt man aber α das in Bezug auf den Modulus 2Δ vollständige Restsystem

$$0, 1, 2 \ldots (2\Delta - 1)$$

durchlaufen, während γ seinen Werth behält, so durchläuft (nach §. 18) der Ausdruck $(a\alpha + b\gamma)$, weil a relative Primzahl gegen den Modulus ist, ebenfalls ein vollständiges Restsystem, und folglich gehören zu jedem solchen geraden γ genau $\varphi(2\Delta)$ erlaubte Werthe von α, wo die Charakteristik φ im frühern Sinne (§. 11) gebraucht ist. Jedem der Δ ungeraden Werthe

$$1, 3 \ldots (2\Delta - 1)$$

von γ entsprechen ebenfalls $\varphi(2\Delta)$ erlaubte Werthe von α; dies leuchtet unmittelbar ein, wenn Δ gerade ist, weil die Forderung sich dann ebenfalls darauf reducirt, dass $(a\alpha + b\gamma)$ relative Primzahl gegen 2Δ werden muss. Ist aber Δ und also auch $\pm\Delta\gamma^2$ ungerade, so muss, da

$$(a\alpha + b\gamma)^2 \pm \Delta\gamma^2$$

ungerade und relative Primzahl gegen Δ werden soll, $(a\alpha + b\gamma)$ gerade und relative Primzahl gegen Δ werden, und folglich muss auch der Rest von $(a\alpha + b\gamma)$ in Bezug auf den Modul 2Δ gerade und relative Primzahl gegen Δ sein, und umgekehrt wird, sobald dies der Fall ist, die obige Forderung erfüllt sein. Durchläuft nun α alle seine 2Δ Werthe, so durchläuft der Rest von $(a\alpha + b\gamma)$ dieselben 2Δ Werthe; unter diesen sind die folgenden Δ Reste gerade

$$0,\ 2,\ 4\ \ldots\ 2(\Delta - 1),$$

und unter diesen sind $\varphi(\Delta)$ relative Primzahlen gegen die ungerade Zahl Δ. Dies ist also die Anzahl der zu jedem ungeraden γ gehörenden erlaubten Werthe von α; da nun aber Δ ungerade, also relative Primzahl gegen 2 ist, so ist auch $\varphi(2\Delta) = \varphi(2)\varphi(\Delta) = \varphi(\Delta)$, und folglich haben wir in allen Fällen dieselbe Antwort: zu jedem geraden oder ungeraden γ gehören stets $\varphi(2\Delta)$ erlaubte Werthe von α; mithin existiren im Ganzen $2\Delta\varphi(2\Delta)$ erlaubte Combinationen (α, γ).

Zweitens: $\sigma = 2$; a und c gerade, b ungerade, und $D \equiv 1$ (mod. 4). Es fragt sich: für wieviele Combinationen (α, γ) ist

$$\tfrac{1}{2}a\alpha^2 + b\alpha\gamma + \tfrac{1}{2}c\gamma^2$$

ungerade und relative Primzahl gegen Δ? — Wir beschränken uns zunächst darauf, die Combinationen zu bestimmen, für welche dieser Werth ungerade ausfällt. Da wir den Repräsentanten (a, b, c) so gewählt haben, dass $\frac{1}{2}a$ relative Primzahl gegen 2Δ und also auch ungerade ist, so wird

$$D = b^2 - ac \equiv 1 \quad \text{oder} \quad \equiv 5 \pmod{8},$$

je nachdem $\frac{1}{2}c$ gerade oder ungerade ist; im ersten Fall muss daher $\alpha(\frac{1}{2}a\alpha + b\gamma)$ ungerade, also α ungerade, und γ gerade sein; im zweiten Fall muss mindestens eine der beiden Zahlen α und γ ungerade sein. Die Anzahl der erlaubten Combinationen ist hierdurch im ersten Falle auf Δ^2, im zweiten auf $3\Delta^2$ herabgedrückt.

Soll nun der Werth von $\frac{1}{2}a\alpha^2 + b\alpha\gamma + \frac{1}{2}c\gamma^2$ auch relative Primzahl gegen Δ werden, so ist erforderlich und hinreichend, dass

$$(a\alpha + b\gamma)^2 \pm \Delta\gamma^2 = 2a(\tfrac{1}{2}a\alpha^2 + b\alpha\gamma + \tfrac{1}{2}c\alpha^2)$$

oder also $(a\alpha + b\gamma)$ relative Primzahl gegen Δ werde. Im ersten Fall, wo $D \equiv 1 \pmod{8}$ ist, dürfen für γ nur gerade, für α nur ungerade Werthe gesetzt werden. Giebt man daher γ einen bestimmten der Δ Werthe

$$0, 2, 4 \ldots (2\Delta - 2)$$

und lässt dann α die sämmtlichen Δ Werthe

$$1, 3, 5 \ldots (2\Delta - 1)$$

durchlaufen, welche offenbar in Bezug auf den Modul Δ ein vollständiges Restsystem bilden, so gilt (da a relative Primzahl gegen Δ ist) dasselbe von den Δ entsprechenden Zahlen $(a\alpha + b\gamma)$, und folglich sind unter denselben $\varphi(\Delta) = \varphi(2\Delta)$ relative Primzahlen gegen Δ. Im Ganzen giebt es daher in diesem Fall $\Delta\varphi(2\Delta)$ erlaubte Combinationen (α, γ). — Im zweiten Fall, wo $D \equiv 5 \pmod{8}$ ist, und in welchem mindestens eine der beiden Zahlen α, γ ungerade sein muss, findet man auf dieselbe Weise, dass jedem geraden Werthe von γ wieder $\varphi(\Delta) = \varphi(2\Delta)$ ungerade Werthe von α entsprechen, woraus zunächst $\Delta\varphi(2\Delta)$ zulässige Combinationen entspringen; ist aber γ ungerade, und durchläuft α seine sämmtlichen 2Δ Werthe, so durchläuft der Ausdruck $(a\alpha + b\gamma)$ zweimal dasselbe vollständige Restsystem in Bezug auf den Modulus Δ; es giebt daher immer $2\varphi(\Delta) = 2\varphi(2\Delta)$ erlaubte Werthe von α, so dass aus den Δ ungeraden Werthen von γ genau $2\Delta\varphi(2\Delta)$ erlaubte Combinationen (α, γ) entspringen. Im Ganzen giebt es daher in diesem zweiten Falle $3\Delta\varphi(2\Delta)$ erlaubte Combinationen (α, γ).

Wir können die sämmtlichen Fälle so zusammenfassen: die Anzahl der Paare von zusammengehörigen arithmetischen Reihen

$$x = 2\Delta v + \alpha, \quad y = 2\Delta w + \gamma$$

welche der Bedingung I. genügen, ist

$$= \omega . \Delta\varphi(2\Delta),$$

wo

$$\omega = 2, \text{ wenn } \sigma = 1$$
$$\omega = 1, \text{ wenn } \sigma = 2 \text{ und } D \equiv 1 \pmod{8}$$
$$\omega = 3, \text{ wenn } \sigma = 2 \text{ und } D \equiv 5 \pmod{8}$$

ist.

§. 95.

Wir kehren nun zu unserer Hauptgleichung zurück, der wir die Form

$$\varrho \sum \frac{1}{(ax^2+2bxy+cy^2)^{1+\varrho}} + \cdots = \frac{\varrho \varkappa}{\sigma^{1+\varrho}} \sum \frac{1}{n^{1+\varrho}} \sum \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}}$$

geben, indem wir $s = 1 + \varrho$ setzen, mit ϱ multipliciren und durch $\sigma^{1+\varrho}$ dividiren; lassen wir jetzt die positive Zahl ϱ unendlich klein werden, so haben wir die Grenzwerthe der einzelnen Glieder zu bestimmen, welche sich auf der linken und rechten Seite befinden. Indem wir mit der Discussion der linken Seite beginnen, wird es wieder nothwendig, den Fall einer negativen Determinante von dem einer positiven vollständig zu trennen.

Wir nehmen daher zunächst an, die Determinante D sei *negativ* $= -\varDelta$. Dann sind die Variabeln x, y in der der Form (a, b, c) entsprechenden Hauptsumme nur der Bedingung I. unterworfen, und wir haben eben gesehen, dass eine solche Hauptsumme in $\omega\varDelta\varphi(2\varDelta)$ Partialreihen zerfällt, welche den einzelnen zulässigen Combinationen (α, γ) entsprechen. Betrachten wir daher zunächst nur eine einzige solche Partialsumme

$$\varrho \sum \frac{1}{(ax^2+2bxy+cy^2)^{1+\varrho}},$$

in welcher x, y alle Werthe

$$x = 2\varDelta v + \alpha, \quad y = 2\varDelta w + \gamma$$

zu durchlaufen haben, die einer bestimmten zulässigen Combination (α, γ) und allen denkbaren ganzzahligen Werthen v, w entsprechen. Nach den in den Supplementen (II. §. 118) aufgestellten Principien ist der Grenzwerth des vorstehenden Productes identisch mit dem des Quotienten $T:t$, wo t eine über alle Grenzen wachsende positive Zahl, und T die zugehörige Anzahl der dargestellten Zahlen $ax^2 + 2bxy + cy^2$ bedeutet, welche nicht grösser als t sind, für welche also

$$a\left(\frac{x}{\sqrt{t}}\right)^2 + 2b\frac{x}{\sqrt{t}} \cdot \frac{y}{\sqrt{t}} + c\left(\frac{y}{\sqrt{t}}\right)^2 \leqq 1$$

ist. Dieser Grenzwerth des Quotienten $T:t$ lässt sich leicht mit

Hülfe einer geometrischen Betrachtung bestimmen; setzt man nämlich

$$\frac{x}{\sqrt{t}} = \xi, \quad \frac{y}{\sqrt{t}} = \eta,$$

so ist T die Anzahl der Werthenpaare

$$\xi = \frac{2\Delta}{\sqrt{t}} v + \frac{\alpha}{\sqrt{t}}, \quad \eta = \frac{2\Delta}{\sqrt{t}} w + \frac{\gamma}{\sqrt{t}}, \tag{1}$$

für welche

$$a\xi^2 + 2b\xi\eta + c\eta^2 \leqq 1 \tag{2}$$

wird; sieht man nun ξ, η als rechtwinklige Coordinaten eines Punctes in einer Ebene an, und lässt man v und w alle ganzzahligen Werthe durchlaufen, so bilden die durch die Formeln (1) bestimmten Puncte (ξ, η) ein Gitter, welches durch die rechtwinklige Kreuzung zweier Systeme von Geraden entsteht, die den Axen parallel sind, und von denen je zwei benachbarte die constante Distanz $\delta = 2\Delta : \sqrt{t}$ haben. Die ganze Ebene wird auf diese Weise in Quadrate von dem Flächeninhalt

$$\delta^2 = \frac{4\Delta^2}{t}$$

zerlegt, deren Eckpuncte jene Puncte (ξ, η) sind; und folglich ist T die Anzahl derjenigen dieser Gitterpuncte (ξ, η), welche nicht ausserhalb der durch die Gleichung

$$a\xi^2 + 2b\xi\eta + c\eta^2 = 1 \tag{3}$$

dargestellten Curve liegen; da nun $b^2 - ac = -\Delta$ negativ (und a positiv) ist, so ist diese Curve eine Ellipse, deren Mittelpunct mit dem Nullpunct des Coordinatensystems zusammenfällt. Nach einem ebenfalls in den Supplementen (III. §. 120) aufgestellten Hülfssatz hat folglich das Product

$$T . \delta^2 = 4\Delta^2 . \frac{T}{t}$$

den Flächeninhalt A dieser Ellipse zum Grenzwerth, wenn t unendlich gross und also δ unendlich klein wird; es ist daher der gesuchte Grenzwerth

$$\lim \frac{T}{t} = \frac{A}{4\Delta^2},$$

woraus schon folgt, dass derselbe von (α, γ) unabhängig und also für jede der $\omega \Delta \varphi(2\Delta)$ Partialsummen, welche unsere Hauptsumme

constituiren, derselbe ist. Mithin ist der Grenzwerth dieser der Form (a, b, c) entsprechenden Hauptsumme

$$\varrho \sum \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}}$$

gleich

$$\omega \Delta \varphi(2\Delta) \cdot \frac{A}{4\Delta^2} = \frac{\omega \varphi(2\Delta)}{4\Delta} A,$$

wo A den Flächeninhalt der Ellipse (3) bezeichnet*). Um diesen zu bestimmen, transformire man die Gleichung der Ellipse durch Einführung solcher rechtwinkliger Coordinaten, welche mit den Hauptaxen der Ellipse zusammenfallen, wodurch sie die Form

$$a'\xi'^2 + c'\eta'^2 = 1$$

annehmen wird. Bekanntlich bleibt bei einer solchen orthogonalen Transformation die Determinante $b^2 - ac$ ungeändert, so dass

$$a'c' = ac - b^2 = \Delta$$

ist; andererseits sind $\sqrt{a'}$ und $\sqrt{c'}$ die reciproken Werthe der beiden Halbaxen, und folglich ist

$$A = \frac{\pi}{\sqrt{a'c'}} = \frac{\pi}{\sqrt{\Delta}},$$

wo natürlich die Quadratwurzel *positiv* zu nehmen ist. Es ergiebt sich also das merkwürdige Resultat, dass dieser Flächeninhalt A, und folglich auch der obige Grenzwerth

$$\frac{\omega \pi \varphi(2\Delta)}{4\Delta\sqrt{\Delta}}$$

der auf die eine Form (a, b, c) bezüglichen Hauptsumme von den einzelnen Coefficienten a, b, c und folglich von der individuellen Natur dieser Form gänzlich unabhängig ist. Denselben Grenzwerth wird daher jede andere, einer andern Form (a', b', c') des Systems S entsprechende, Hauptsumme haben; bezeichnen wir daher mit h die Anzahl dieser einzelnen Hauptsummen auf der linken Seite unserer Gleichung, d. h. also die *Anzahl der Classen nicht äquivalenter ursprünglicher Formen der σten Art für die negative De-*

---

*) Daraus, dass der Quotient $T : t$ sich einem bestimmten Grenzwerth nähert, geht zufolge des in den Supplementen (II. §. 118) aufgestellten Satzes nachträglich hervor, dass die bisher betrachteten unendlichen Reihen für jeden positiven Werth von ϱ, also für alle Werthe $s > 1$ convergiren.

terminante $D = -\Delta$, so wird der Grenzwerth der ganzen linken Seite gleich

$$\frac{\omega\pi\varphi(2\Delta)}{4\Delta\sqrt{\Delta}}h.$$

§. 96.

Gehen wir nun zur rechten Seite der Gleichung über, so haben wir wieder mit Hülfe der in den Supplementen (II. §. 117) aufgestellten Principien den Grenzwerth des Productes

$$\varrho\,\Sigma\,\frac{1}{n^{1+\varrho}}$$

zu ermitteln, wo das Summenzeichen sich auf alle positiven ganzen Zahlen n bezieht, die relative Primzahlen gegen 2Δ sind. Bezeichnet man nun mit ν, ν', ν''... die $\varphi(2\Delta)$ ersten dieser Zahlen, nämlich diejenigen, welche $< 2\Delta$ sind, so kann man die vorstehende Summe in $\varphi(2\Delta)$ Partialsummen von der Form

$$\varrho\left\{\frac{1}{\nu^{1+\varrho}}+\frac{1}{(\nu+2\Delta)^{1+\varrho}}+\frac{1}{(\nu+4\Delta)^{1+\varrho}}+\frac{1}{(\nu+6\Delta)^{1+\varrho}}+\cdots\right\}$$

zerlegen, in welcher die unter dem Exponenten $(1+\varrho)$ stehenden Zahlen jedesmal eine arithmetische Reihe von der Differenz 2Δ bilden; da nun nach dem in den Supplementen behandelten speciellen Fall der Grenzwerth einer solchen Partialreihe

$$=\frac{1}{2\Delta}$$

und also unabhängig von ν ist, so wird der Grenzwerth der ganzen Summe

$$=\frac{\varphi(2\Delta)}{2\Delta},$$

und mithin wird der Grenzwerth der ganzen rechten Seite der Hauptgleichung

$$\frac{\varkappa\varphi(2\Delta)}{\sigma.2\Delta}\lim\Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}}.$$

Da aber beide Seiten für jeden Werth von $s > 1$, d. h. für jeden positiven Werth von ϱ identisch sind, und da sie folglich, wenn überhaupt einen, nothwendig denselben Grenzwerth haben müssen,

so ergiebt sich aus der Vergleichung, indem wir $D = -\varDelta$ restituiren,

$$h = \frac{2\varkappa}{\sigma\omega\pi}\sqrt{-D}\,.\,\lim \Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}}$$

als Ausdruck für die Classenanzahl der ursprünglichen Formen σter Art (mit positiven äusseren Coefficienten) für eine *negative* Determinante D; hierin ist ferner (nach §. 88)

$\varkappa = 4$, wenn $D = -1$,
$\varkappa = 6$, wenn $D = -3$ und $\sigma = 2$,
$\varkappa = 2$ in den übrigen Fällen;

und (nach §. 94)

$\omega = 2$, wenn $\sigma = 1$,
$\omega = 1$, wenn $\sigma = 2$ und $D \equiv 1 \pmod{8}$,
$\omega = 3$, wenn $\sigma = 2$ und $D \equiv 5 \pmod{8}$.

§. 97.

Für Formen der ersten Art erhalten wir daher, indem wir $\sigma = 1$, $\varkappa = 2$ und $\omega = 2$ setzen,

$$h = \frac{2}{\pi}\sqrt{-D}\,.\,\lim \Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}},$$

mit Ausnahme des einzigen Falles $D = -1$, in welchem $\varkappa$ nicht $= 2$, sondern $= 4$ ist, und folglich

$$h = \frac{4}{\pi}\lim \Sigma\frac{(-1)^{\frac{1}{2}(n-1)}}{n^{1+\varrho}}$$

wird; es wird später (§. 101) allgemein gezeigt werden, dass

$$\lim \Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}} = \Sigma\left(\frac{D}{n}\right)\frac{1}{n}$$

ist, vorausgesetzt, dass auf der rechten Seite die Glieder ihrer Grösse nach geordnet werden; in dem speciellen Fall $D = -1$ wird daher

$$h = \frac{4}{\pi}\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots\right) = 1,$$

da der Werth der in der Parenthese befindlichen unendlichen Reihe von *Leibnitz* bekanntlich $= \frac{1}{4}\pi$ ist; hierin liegt also eine Bestätigung unserer Principien, da in der That für die Determi-

nante $D = -1$ nur eine einzige Classe von Formen (mit positiven äusseren Coefficienten) existirt.

Wir wollen nun mit der vorstehenden Formel für die Classenanzahl h der Formen der ersten Art die für die Anzahl h' der Formen der zweiten Art vergleichen. Wir unterscheiden zu dem Zweck die beiden Fälle, in welchen $D \equiv 1$ oder $D \equiv 5 \pmod{8}$ ist. Im ersten Fall ist $\varkappa = 2$ und $\omega = 1$, folglich

$$h' = \frac{2}{\pi}\sqrt{-D} \,.\, \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}} = h;$$

im zweiten Fall dagegen ist $\omega = 3$ und $\varkappa = 2$, also

$$h' = \frac{1}{3} \cdot \frac{2}{\pi}\sqrt{-D} \,.\, \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}} = \frac{1}{3} h,$$

ausgenommen den einzigen Fall $D = -3$, in welchem $\varkappa$ nicht $= 2$, sondern $= 6$, und folglich wieder

$$h' = h$$

ist. Wir können daher so zusammenfassen: es ist

$h' = h$, wenn $D \equiv 1 \pmod{8}$, und für $D = -3$;

$h' = \frac{1}{3} h$, wenn $D \equiv 5 \pmod{8}$, ausgenommen $D = -3$.

Diese Beziehungen zwischen der Anzahl der Formen der ersten und der zweiten Art hat schon *Gauss* gefunden, aber auf einem ganz andern Wege*).

§. 98.

Wir haben nun dieselbe Untersuchung für den Fall einer *positiven* Determinante $D = \Delta$ zu wiederholen. Betrachten wir zunächst die linke Seite, so zerlegen wir wieder jede auf eine bestimmte Form (a, b, c) bezügliche Hauptsumme in $\omega \Delta \varphi(2\Delta)$ Partialsummen von der Form

$$\varrho \Sigma \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}},$$

in deren jeder die Summationsbuchstaben alle Werthenpaare

$$x = 2\Delta v + \alpha, \quad y = 2\Delta w + \gamma \qquad (1)$$

zu durchlaufen haben, die einer bestimmten Combination (α, γ)

*) *D. A.* art. 256 VI. — Vergl. §. 151, I.

und allen ganzzahligen Werthen v, w entsprechen; jetzt aber treten ausserdem noch die Isolirungsbedingungen II. hinzu, denen gemäss

$$y \geqq 0, \quad ax + by > \frac{T}{U} y \tag{2}$$

sein soll. Diese letzteren Bedingungen haben, wie wir schon früher gesehen haben (§. 87), zur Folge, dass

$$ax + (b + \sqrt{D})y, \quad ax + (b - \sqrt{D})y,$$

und also auch

$$ax^2 + 2bxy + cy^2$$

positive Zahlen sind, und wir können daher wieder die in den Supplementen aufgestellten Principien anwenden; bezeichnen wir mit t einen beliebigen positiven Werth und mit τ die Anzahl derjenigen in den Reihen (1) enthaltenen und zugleich den Bedingungen (2) genügenden Werthenpaare x, y, für welche

$$ax^2 + 2bxy + cy^2 \leqq t \tag{3}$$

ist, so haben wir nur den Grenzwerth des Quotienten $\tau : t$ für unbegrenzt wachsende Werthe von t zu bestimmen, um dadurch zugleich den Grenzwerth der obigen Partialsumme zu finden, welche der einen Combination (α, γ) entspricht. Setzen wir wieder (indem wir $\sqrt{t}$ positiv nehmen)

$$\xi = \frac{x}{\sqrt{t}}, \quad \eta = \frac{y}{\sqrt{t}},$$

und sehen wir ξ, η als rechtwinklige Coordinaten eines Punctes einer Ebene an, so ist τ die Anzahl derjenigen in der Doppelreihe

$$\xi = \frac{2\Delta}{\sqrt{t}} v + \frac{\alpha}{\sqrt{t}}, \quad \eta = \frac{2\Delta}{\sqrt{t}} w + \frac{\gamma}{\sqrt{t}}$$

enthaltenen Gitterpuncte, welche den drei Ungleichheiten

$$\eta \geqq 0, \quad a\xi + b\eta > \frac{T}{U} \eta,$$

$$a\xi^2 + 2b\xi\eta + c\eta^2 \leqq 1$$

Genüge leisten, d. h. welche innerhalb eines Stückes der $\xi\eta$-Ebene liegen, das zum Theil durch die Axe der ξ, zum Theil durch eine durch den Nullpunct gehende Gerade, und endlich durch eine Hyperbel begrenzt wird, die den Nullpunct zum Mittelpuncte hat. Bezeichnen wir mit B den Flächeninhalt dieses Stückes der $\xi\eta$-Ebene, so wird nach den in den Supplementen aufgestellten Principien, wenn t unendlich gross, und also die Kante $\delta = 2\Delta : \sqrt{t}$ der Gitterquadrate unendlich klein wird,

$$\lim \tau . \delta^2 = 4\varDelta^2 . \lim \frac{\tau}{t} = B,$$

also

$$\lim \frac{\tau}{t} = \frac{B}{4\varDelta^2}$$

sein. Da dieser Grenzwerth zugleich der Grenzwerth der Partialsumme ist, welche sich auf die eine Combination (α, γ) bezieht, so wird, da hierin die Werthe α, γ ganz herausgefallen sind, jede der $\omega \varDelta \varphi(2\varDelta)$ Partialsummen, welche den verschiedenen Combinationen (α, γ) entsprechen, und welche zusammen die auf die Form (a, b, c) bezügliche Hauptsumme constituiren, denselben Grenzwerth haben; und mithin wird

$$\frac{\omega \varphi(2\varDelta)}{4\varDelta} B$$

der Grenzwerth der ganzen Hauptsumme

$$\varrho \sum \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}}$$

sein. Um nun den Flächeninhalt B des durch die drei obigen Ungleichheiten definirten Hyperbelsectors zu finden, wird man am besten Polarcoordinaten r, φ einführen, indem man

$$\xi = r\cos\varphi, \quad \eta = r\sin\varphi$$

setzt, wo, wie gewöhnlich, r stets positiv und φ zwischen 0 und 2π genommen werden soll, was hinreicht, um jeden Punct (ξ, η) der Ebene einmal und nur einmal zu erzeugen. Durch diese Transformation verwandeln sich die früheren Grenzbedingungen in folgende:

$$\sin\varphi \geqq 0; \quad a \operatorname{cotang}\varphi + b > \frac{T}{U};$$

$$r^2 (a\cos\varphi^2 + 2b\cos\varphi\sin\varphi + c\sin\varphi^2) \leqq 1,$$

und wir wiederholen die frühere Bemerkung, dass für jeden, den beiden ersten Bedingungen genügenden Winkel φ die Grössen

$$a\cos\varphi + (b + \sqrt{D})\sin\varphi, \quad a\cos\varphi + (b - \sqrt{D})\sin\varphi,$$
$$a\cos\varphi^2 + 2b\cos\varphi\sin\varphi + c\sin\varphi^2$$

positiv sind, so dass also innerhalb des durch diese beiden ersten Bedingungen begrenzten Winkelraumes keine Asymptote, sondern nur ein endliches Stück der Hyperbel liegt, woraus schon folgt,

dass der entsprechende Sector jedenfalls einen endlichen Werth hat*). Dieser wird bekanntlich durch die Formel

$$B = \int\int r dr d\varphi = \tfrac{1}{2}\int r^2 d\varphi$$

gefunden, wo nun in dem einfachen Integral rechts für r^2 der in der Peripherie der Hyperbel geltende Werth

$$r^2 = \frac{1}{a\cos\varphi^2 + 2b\cos\varphi\sin\varphi + c\sin\varphi^2}$$

$$= \frac{a}{2\sqrt{D}}\left\{\frac{1}{a\,\mathrm{cotang}\,\varphi + b - \sqrt{D}} - \frac{1}{a\,\mathrm{cotang}\,\varphi + b + \sqrt{D}}\right\}\frac{1}{\sin\varphi^2}$$

zu setzen ist; wir erhalten daher, indem wir $\mathrm{cotang}\,\varphi$ als neue Variabele betrachten, und

$$\frac{d\varphi}{\sin\varphi^2} = -\,d\,\mathrm{cotang}\,\varphi$$

setzen, das unbestimmte Integral

$$\frac{1}{2}\int r^2 d\varphi$$

$$= \frac{1}{4\sqrt{D}}\int\frac{a\,d\,\mathrm{cotang}\,\varphi}{a\,\mathrm{cotang}\,\varphi + b + \sqrt{D}} - \frac{1}{4\sqrt{D}}\int\frac{a\,d\,\mathrm{cotang}\,\varphi}{a\,\mathrm{cotang}\,\varphi + b - \sqrt{D}}$$

$$= \frac{1}{4\sqrt{D}}\log\frac{a\,\mathrm{cotang}\,\varphi + b + \sqrt{D}}{a\,\mathrm{cotang}\,\varphi + b - \sqrt{D}};$$

diese Integration ist aber auszudehnen über alle Werthe von φ, welche einen positiven Sinus haben, also von $\varphi = 0$ ab bis zu dem Werth, wo $U(a\,\mathrm{cotang}\,\varphi + b) = T$ wird; dieser Endwerth von φ ist durch die Bedingung, dass $\sin\varphi$ positiv sein soll, vollständig bestimmt, und wir haben schon oben darauf hingewiesen, dass innerhalb dieses ganzen Winkelraums die beiden Grössen

$$a\,\mathrm{cotang}\,\varphi + b + \sqrt{D},\quad a\,\mathrm{cotang}\,\varphi + b - \sqrt{D}$$

stets das positive Zeichen behalten, so dass das obige unbestimmte Integral eine stetige reelle Function von φ ist, woraus folgt, dass wir nur die beiden Grenzen in dasselbe einzusetzen haben. Auf diese Weise erhalten wir

$$B = \frac{1}{4\sqrt{D}}\log\frac{T + U\sqrt{D}}{T - U\sqrt{D}} = \frac{1}{2\sqrt{D}}\log\frac{T + U\sqrt{D}}{\sigma}.$$

*) Hieraus folgt wieder nachträglich die Convergenz der bisher betrachteten Reihen für jeden positiven Werth von ϱ, d. h. für jeden Werth von $s > 1$.

Der Grenzwerth der auf die Form $(a, b, c)'$ bezüglichen Hauptsumme wird daher, wenn man statt Δ wieder D schreibt, gleich

$$\frac{\omega\varphi(2D)}{8D\sqrt{D}}\log\frac{T+U\sqrt{D}}{\sigma},$$

wo, wie früher, T, U die beiden kleinsten der unbestimmten Gleichung $T^2 - DU^2 = \sigma^2$ genügenden positiven Zahlen bedeuten. Mithin zeigt sich auch hier, wie früher bei den Formen von negativer Determinante, dass der Grenzwerth einer auf eine einzelne Form (a, b, c) des Systems S bezüglichen Hauptsumme nur von der Determinante D (und der Art σ), dagegen gar nicht von dem individuellen Charakter der Form abhängt, dass er also für alle diese Formen derselbe ist. Bezeichnen wir wieder mit h die Anzahl aller in S enthaltenen Formen, d. h. die *Anzahl aller Classen ursprünglicher Formen σter Art für die positive Determinante D*, so ist daher

$$h\frac{\omega\varphi(2D)}{8D\sqrt{D}}\log\frac{T+U\sqrt{D}}{\sigma}$$

der Grenzwerth, welchem für unendlich abnehmende positive Werthe von ϱ die linke Seite unserer Hauptgleichung sich nähert. Auf der rechten Seite ist $\varkappa = 1$, ferner ebenso wie früher bei Formen von negativer Determinante

$$\lim \varrho \sum \frac{1}{n^{1+\varrho}} = \frac{\varphi(2\Delta)}{2\Delta} = \frac{\varphi(2D)}{2D},$$

und folglich erhalten wir durch Vergleichung beider Seiten der Hauptgleichung das Resultat

$$h = \frac{1}{\sigma\omega}\cdot\frac{4\sqrt{D}}{\log\dfrac{T+U\sqrt{D}}{\sigma}}\cdot\lim\sum\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}}.$$

§. 99.

Für Formen der ersten Art ist $\sigma = 1$, und $\omega = 2$ (§. 94); hieraus folgt für die Anzahl der Classen ursprünglicher Formen erster Art der Ausdruck

$$h = \frac{2\sqrt{D}}{\log(T+U\sqrt{D})}\cdot\lim\sum\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}},$$

wo T, U die kleinsten der Gleichung

$$T^2 - D U^2 = 1$$

genügenden positiven ganzen Zahlen bedeuten. Ist ferner $D \equiv 1$ (mod. 4), so existiren auch Formen der zweiten Art, deren Anzahl wir mit h' bezeichnen wollen; es ist dann $\sigma = 2$, und $\omega = 1$ oder $= 3$ zu setzen, je nachdem $D \equiv 1$ (mod. 8) oder $\equiv 5$ (mod. 8) ist; wir erhalten daher, wenn wir zur Unterscheidung mit T', U' die kleinsten der unbestimmten Gleichung

$$T'^2 - D U'^2 = 4$$

genügenden ganzen positiven Zahlen bezeichnen,

$$h' = \frac{1}{\omega} \cdot \frac{2\sqrt{D}}{\log\frac{1}{2}(T' + U'\sqrt{D})} \cdot \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}}.$$

Nun ist einleuchtend, dass jede Auflösung (t, u) der Gleichung $t^2 - Du^2 = 1$ durch Verdoppelung eine Auflösung $(t' = 2t, u' = 2u)$ der Gleichung $t'^2 - Du'^2 = 4$ giebt, und umgekehrt, dass man durch Halbirung jeder *geraden* Auflösung (t', u') der letztern eine Auflösung (t, u) der erstern erhält. Hieraus folgt unmittelbar, dass $(t' = 2T, u' = 2U)$ jedenfalls die kleinste gerade Auflösung der Gleichung $t'^2 - Du'^2 = 4$ ist. Ist nun zunächst $D \equiv 1$ (mod. 8), so kann diese Gleichung überhaupt nur gerade Auflösungen haben; denn wäre eine der beiden Zahlen t', u' und folglich auch die andere ungerade, so wäre die linke Seite durch 8 theilbar, während sie doch $= 4$ sein soll; in diesem Fall ist daher

$$T' = 2T, \quad U' = 2U, \quad \frac{T' + U'\sqrt{D}}{2} = T + U\sqrt{D},$$

und da ausserdem $\omega = 1$ ist, so ergiebt sich

$$h' = h, \quad \text{wenn } D \equiv 1 \text{ (mod. 8)}.$$

Im andern Fall $D \equiv 5$ (mod. 8) kann die Regel nicht so bestimmt ausgesprochen werden, indem bei manchen dieser Determinanten die kleinste Auflösung (T', U') wieder eine gerade, bei anderen aber eine ungerade ist. Im ersten dieser beiden Fälle ist dann wieder $T' = 2T$, $U' = 2U$ und folglich, da $\omega = 3$ ist,

$$h' = \tfrac{1}{3}h, \text{ wenn } D \equiv 5 \text{ (mod. 8), und } T', U' \text{ gerade};$$

es giebt unterhalb 200 nur 5 Determinanten, nämlich 37, 101, 141, 189, 197, für welche dieser Fall eintritt*).

*) Vergl. *Cayley: Note sur l'équation* $x^2 - Dy^2 = \pm 4$, $D \equiv 5$ (mod. 8), Crelle's Journal LIII. p. 369. Man findet daselbst eine Tabelle, welche bis $D = 997$ reicht.

Im zweiten Falle, wenn T', U' ungerade sind, haben wir unter allen positiven Auflösungen (t', u'), welche (§. 85) aus der Formel

$$\frac{t' + u'\sqrt{D}}{2} = \left(\frac{T' + U'\sqrt{D}}{2}\right)^n$$

für positive Werthe von n entspringen, die kleinste gerade aufzusuchen. Versuchen wir daher die nächst grössere Auflösung, welche dem Exponenten $n = 2$ entspricht, so erhalten wir

$$t' = \frac{T'^2 + DU'^2}{2}, \quad u' = T'U';$$

da u' offenbar ungerade ist, so gehen wir zu dem folgenden Exponenten $n = 3$ über, um die nächst grössere Auflösung zu prüfen; da finden wir

$$t' = \frac{T'^3 + 3DT'U'^2}{4} = T'\,\frac{T'^2 + 3DU'^2}{4},$$

und da

$$T'^2 \equiv U'^2 \equiv 1 \pmod{8}, \quad 3D \equiv -1 \pmod{8}$$

ist, so folgt, dass t' und folglich auch u' gerade Zahlen werden, und also $t' = 2T$, $u' = 2U$ ist. Wir haben daher in diesem Falle

$$T + U\sqrt{D} = \left(\frac{T' + U'\sqrt{D}}{2}\right)^3$$

und

$$\log\frac{T' + U'\sqrt{D}}{2} = \tfrac{1}{3}\log(T + U\sqrt{D});$$

berücksichtigt man ferner, dass $\omega = 3$ ist, so ergiebt sich die Relation

$$h' = h, \quad \text{wenn } D \equiv 5 \pmod{8}, \quad \text{und } T',\ U' \text{ ungerade.}$$

Auch für positive Determinanten hat *Gauss**) ebenfalls die Relationen zwischen den Anzahlen der Formen der ersten und zweiten Art aufgestellt, für den letzten Fall aber, in welchem $D \equiv 5 \pmod{8}$ ist, in ganz anderer Form; er zeigt nämlich, dass die drei ursprünglichen Formen

$$(1,\ 0,\ -D),\ \left(4,\ 1,\ \frac{1-D}{4}\right),\ \left(4,\ 3,\ \frac{9-D}{4}\right)$$

entweder alle äquivalent sind, oder drei verschiedenen Classen angehören; und je nachdem das Erstere oder Letztere eintritt, ist $h' = h$ oder $h' = \frac{1}{3}h$.

*) *D. A.* art. 256. VI. — Vergl. §. 151, I.

§. 100.

Nachdem wir im Vorhergehenden für alle Fälle gezeigt haben, wie die Classenanzahl der Formen zweiter Art aus der der Formen erster Art gefunden werden kann, beschränken wir die fernere Untersuchung lediglich auf die Bestimmung der letztern. Bevor wir aber dazu übergehen, können wir eine weitere Zurückführung unserer Aufgabe vornehmen, indem wir zeigen, dass man nur solche Determinanten D zu betrachten braucht, welche durch keine Quadratzahl (ausser 1) theilbar sind.

Ist D eine beliebige Determinante, so kann man immer $D = D' S^2$ setzen, wo S^2 das grösste*) in D aufgehende Quadrat, und also D' ein Product aus lauter ungleichen Primzahlen (oder auch $= -1$) ist, welches dem Zeichen nach mit D übereinstimmt; dann lässt sich die Classenanzahl der Formen von der Determinante D auf die der Formen von der Determinante D' zurückführen. Bezeichnen wir alle auf die Determinante D' bezüglichen Grössen durch beigesetzte Accente, so wollen wir zunächst die beiden Summen

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} \quad \text{und} \quad \Sigma \left(\frac{D'}{n'}\right) \frac{1}{n'^s}$$

mit einander vergleichen, in welchen wir der Bequemlichkeit halber s statt $1 + \varrho$ geschrieben haben. In der zweiten muss der Buchstabe n' alle positiven Zahlen durchlaufen, welche relative Primzahlen gegen $2D'$ sind. Bezeichnen wir mit q' alle positiven ungeraden nicht in D' aufgehenden, und, wie früher, mit q alle positiven ungeraden nicht in D aufgehenden Primzahlen, so ist, wie wir früher gesehen haben,

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s} = \Pi \frac{1}{1 - \left(\frac{D}{q}\right) \frac{1}{q^s}}$$

und natürlich ebenso

$$\Sigma \left(\frac{D'}{n'}\right) \frac{1}{n'^s} = \Pi \frac{1}{1 - \left(\frac{D'}{q'}\right) \frac{1}{q'^s}}.$$

*) Die folgende Untersuchung gilt auch für den Fall, dass D' selbst noch quadratische Factoren hat.

Offenbar bildet nun das System der Primzahlen q nur einen Theil der Primzahlen q', denn eine in $D = D'S^2$ nicht aufgehende Primzahl q geht auch nicht in D' auf und ist folglich eine der Primzahlen q'. Das System der Primzahlen q' besteht daher aus dem der Primzahlen q und aus solchen ungeraden Primzahlen r, welche nicht in D', wohl aber in D, also auch in S aufgehen, und deren Anzahl offenbar endlich ist. Das auf die Determinante D' bezügliche unendliche Product wird sich daher in folgender Weise zerlegen

$$\Pi \frac{1}{1-\left(\frac{D'}{q'}\right)\frac{1}{q'^s}} = \Pi \frac{1}{1-\left(\frac{D'}{q}\right)\frac{1}{q^s}} \cdot \Pi \frac{1}{1-\left(\frac{D'}{r}\right)\frac{1}{r^s}};$$

da nun ferner $D = D'S^2$ und folglich

$$\left(\frac{D}{q}\right) = \left(\frac{D'S^2}{q}\right) = \left(\frac{D'}{q}\right)$$

ist, so erhalten wir, indem wir statt der beiden unendlichen Producte wieder die unendlichen Reihen aufschreiben, das Resultat

$$\Sigma \left(\frac{D}{n}\right)\frac{1}{n^s} = \Sigma \left(\frac{D'}{n'}\right)\frac{1}{n'^s} \cdot \Pi \left(1-\left(\frac{D'}{r}\right)\frac{1}{r^s}\right)$$

und hieraus

$$\lim \Sigma \left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}} = \Pi \left(1-\left(\frac{D'}{r}\right)\frac{1}{r}\right) \lim \Sigma \left(\frac{D'}{n'}\right)\frac{1}{n'^{1+\varrho}},$$

wo also das Productzeichen sich auf alle ungeraden in S, aber nicht in D' aufgehenden Primzahlen r bezieht.

Nachdem wir so für positive wie negative Determinanten das Verhältniss zwischen den beiden analogen Grenzwerthen bestimmt haben, die als Factoren in den Classenanzahlen h und h' für die Determinanten D und D' auftreten, müssen wir wieder die beiden Hauptfälle von einander trennen.

Ist zunächst D' und folglich auch D *negativ*, so haben wir (da wir uns auf Formen der ersten Art beschränken)

$$h = \frac{2\sqrt{-D}}{\pi} \lim \Sigma \left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}}$$

und, den einzigen Fall ausgenommen, in welchem $D' = -1$,

$$h' = \frac{2\sqrt{-D'}}{\pi} \lim \Sigma \left(\frac{D'}{n'}\right)\frac{1}{n'^{1+\varrho}}.$$

Mit Ausnahme des Falles $D' = -1$ ist daher, mit Rücksicht auf

das eben gefundene Verhältniss der beiden Grenzwerthe der unendlichen Reihen,

$$h = h' \times S \,.\, \Pi\left(1 - \left(\frac{D'}{r}\right)\frac{1}{r}\right);$$

ist aber $D' = -1$, also $\varkappa' = 4$, $h' = 1$, und $D = -S^2$ nicht ebenfalls $= -1$, also $S > 1$, so ist die Classenanzahl für eine solche Determinante D gleich

$$\tfrac{1}{2} S \,\Pi\left(1 - \frac{(-1)^{\frac{1}{2}(r-1)}}{r}\right).$$

Für *positive* Determinanten haben wir folgende Formeln erhalten:

$$h = \frac{2\sqrt{D}}{\log(T + U\sqrt{D})} \lim \Sigma \left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}}$$

$$h' = \frac{2\sqrt{D'}}{\log(T' + U'\sqrt{D'})} \lim \Sigma \left(\frac{D'}{n'}\right)\frac{1}{n'^{1+\varrho}}$$

wo T', U' die kleinsten positiven Zahlen bedeuten, die der Gleichung $T'^2 - D'U'^2 = 1$ genügen; hieraus ergiebt sich

$$h = h' \frac{\log(T' + U'\sqrt{D'})}{\log(T + U\sqrt{D})} \times S \,.\, \Pi\left(1 - \left(\frac{D'}{r}\right)\frac{1}{r}\right),$$

und es kommt nur noch darauf an, das Verhältniss der beiden Logarithmen in rationaler Form anzugeben. Offenbar liefert nun jede Lösung (t, u) der Gleichung

$$t^2 - Du^2 = 1, \quad \text{d. h.} \quad t^2 - D'S^2u^2 = 1$$

eine Lösung der Gleichung

$$t'^2 - D'u'^2 = 1,$$

in welcher

$$t' = t, \quad u' = Su,$$

also das zweite Element u' durch S theilbar ist; und umgekehrt, sobald in der Lösung (t', u') das zweite Element u' durch S theilbar ist, so erhält man hieraus eine Lösung der erstern. Hieraus folgt, dass die beiden Zahlen

$$t' = T, \quad u' = SU$$

die kleinste positive Lösung der zweiten Gleichung bilden, in welcher das zweite Element durch S theilbar ist; man kann daher

$$T + SU\sqrt{D'} = T + U\sqrt{D} = (T' + U'\sqrt{D'})^{\lambda}$$

setzen, wo λ der kleinste positive ganze Exponent ist, für welchen der irrationale Bestandtheil der Potenz einen durch S theilbaren Coefficienten erhält; und dann ist

$$h = h' \times \frac{1}{\lambda} \cdot S \cdot \Pi \left(1 - \left(\frac{D'}{r}\right) \frac{1}{r}\right).$$

Setzt man, wie früher,

$$(T' + U' \sqrt{D'})^{\nu} = t'_{\nu} + u'_{\nu} \sqrt{D'},$$

so lässt sich der Werth von λ unmittelbar angeben, wenn für jede einzelne in S aufgehende Primzahl p die kleinste Zahl ν bekannt ist, für welche u'_{ν} durch p theilbar, und zugleich die höchste Potenz von p gegeben ist, welche dann in u'_{ν} aufgeht *); doch gehen wir hierauf nicht weiter ein, da der Hauptzweck, das Verhältniss zwischen den Classenanzahlen h und h' für die Determinanten D und D' zu finden, erreicht ist.

Dieselbe Aufgabe ist, wenigstens für negative Determinanten, auch schon von *Gauss* vollständig gelöst**).

§. 101.

In Folge der vorhergehenden Untersuchungen können wir uns auf den Fall beschränken, in welchem die Determinante D durch kein Quadrat ausser 1 theilbar ist, und es bleibt nur noch übrig, den Grenzwerth der unendlichen Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}}$$

für unendlich abnehmende positive Werthe von ϱ wirklich zu bestimmen.

So lange ϱ positiv bleibt, ist diese Reihe immer convergent, und zwar ist ihre Summe durchaus unabhängig von der Ordnung, in welcher man ihre Glieder auf einander folgen lässt; ist aber $\varrho = 0$, so gehört diese Reihe zu der Classe derjenigen, in welcher die Summe der positiven Glieder für sich, so wie die der negativen Glieder für sich genommen unendlich gross ist. Da nun unter der Summe einer unendlichen convergirenden Reihe stets der Grenzwerth verstanden wird, welchem sich die Summe ihrer *ersten n* Glieder nähert, wenn die Gliederanzahl n unbegrenzt wächst, so sieht man

*) *Dirichlet: Ueber eine Eigenschaft der quadratischen Formen von positiver Determinante* (Crelle's Journal LIII).

**) *D. A.* art. 256. V. — Vergl. §. 151, II. — Die obigen Sätze sind auf anderm Wege auch von *Lipschitz* bewiesen (Crelle's Journal LIII).

leicht ein, dass bei einer unendlichen Reihe von dieser eigenthümlichen Beschaffenheit erst dann von ihrer Convergenz und von ihrer Summe die Rede sein kann, nachdem ihre sämmtlichen Glieder in eine bestimmte *Ordnung* gebracht sind, nach welcher eines auf das andere folgt; denn die Summe, wenn sie überhaupt existirt, hängt wesentlich von der Compensation ab, welche zwischen den für sich allein unendlich wachsenden positiven und negativen Bestandtheilen gerade durch diese Anordnung der Glieder hervorgebracht wird. Eine solche unendliche Reihe hat daher ganz verschiedene Summen, je nach der verschiedenen Anordnung der Glieder. Aber gesetzt auch, dies wäre gar nicht der Fall, sondern die Reihe hätte auch für den Werth $\varrho = 0$ einen vollständig bestimmten Werth, so würde sich immer noch fragen, ob dieser Werth auch der Grenzwerth ist, welchem sich der Werth der Reihe unendlich nähert, wenn ϱ unendlich klein wird, d. h. es würde sich fragen, ob der Werth der unendlichen Reihe sich an der Stelle $\varrho = 0$ *stetig* mit ϱ ändert.

Ueber alle diese Zweifel entscheidet nun der folgende allgemeine Satz*): *Sind $\alpha_1, \alpha_2, \alpha_3 \ldots$ unendlich viele Constanten von der Beschaffenheit, dass die Summe*

$$\beta_n = \alpha_1 + \alpha_2 + \cdots + \alpha_n,$$

wie gross auch n werden mag, ihrem absoluten Werth nach stets kleiner bleibt als eine feste Constante C, so convergirt die unendliche Reihe

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \frac{\alpha_3}{3^s} + \cdots + \frac{\alpha_m}{m^s} + \cdots$$

für jeden positiven Werth des Exponenten s (excl. $s = 0$) und ist zugleich eine stetige Function von s.

Um dies zu beweisen, vergleichen wir die vorstehende Reihe mit der folgenden

$$\beta_1 \left(\frac{1}{1^s} - \frac{1}{2^s}\right) + \beta_2 \left(\frac{1}{2^s} - \frac{1}{3^s}\right) + \beta_3 \left(\frac{1}{3^s} - \frac{1}{4^s}\right) + \cdots$$

Die Summen der ersten n Glieder der erstern und letztern Reihe unterscheiden sich von einander nur um

$$\frac{\beta_n}{(n+1)^s};$$

da nun der Voraussetzung nach β_n seinem absoluten Werth nach

*) *Dirichlet: Recherches etc.* §. 1. — Vergl. §. 143.

stets unterhalb der endlichen Grösse C bleibt, und s positiv ist, so wird dieser Unterschied mit unbegrenzt wachsendem n unendlich klein werden. Nähert sich daher die Summe der ersten n Glieder der einen Reihe einem bestimmten Grenzwerth, d. h. convergirt die eine Reihe, so ist dies auch mit der andern der Fall, und zwar hat sie dieselbe Summe. Wir brauchen daher die obigen Behauptungen nur für die letztere Reihe zu beweisen; dazu betrachten wir die Summe von beliebig vielen Gliedern, welche auf die ersten n Glieder folgen:

$$\beta_{n+1}\left(\frac{1}{(n+1)^s}-\frac{1}{(n+2)^s}\right)+\cdots$$
$$+\beta_{n+m}\left(\frac{1}{(n+m)^s}-\frac{1}{(n+m+1)_s}\right);$$

da die Differenzen

$$\frac{1}{(n+1)^s}-\frac{1}{(n+2)^s},\quad \frac{1}{(n+2)^s}-\frac{1}{(n+3)^s}\cdots$$

sämmtlich positiv sind, und ihre Coefficienten

$$\beta_{n+1},\ \beta_{n+2}\ldots$$

absolut genommen sämmtlich kleiner als C sind, so ist die Summe dieser m Glieder absolut genommen auch kleiner als das Product aus C und der Summe jener m Differenzen, d. h. kleiner als

$$C\left(\frac{1}{(n+1)^s}-\frac{1}{(n+m+1)^s}\right)$$

und folglich auch kleiner als

$$\frac{C}{(n+1)^s}<\frac{C}{n^s};$$

die Summe dieser m Glieder der Reihe kann daher, wie gross ihre Anzahl m auch genommen werden mag, durch hinreichend grosse Werthe von n kleiner gemacht werden, als jeder vorher vorgeschriebene noch so kleine Werth. Das Stattfinden dieser Erscheinung ist aber bekanntlich nicht nur ein erforderliches, sondern auch ein ausreichendes Kennzeichen für die Convergenz einer jeden unendlichen Reihe.

Nachdem so für jeden positiven Werth von s die Convergenz der Reihe gezeigt ist, haben wir noch zu beweisen, dass der Werth der Reihe sich stetig mit s ändert; wir weisen dies nach für das Gebiet aller positiven Werthe von s, die grösser sind als ein bestimmter positiver Werth σ; da man nämlich, wie klein ein von

Null verschiedener positiver Werth s auch sein mag, immer noch einen positiven Werth σ angeben kann, welcher unterhalb s liegt, so wird der Beweis dann wirklich für alle positiven Werthe s (excl. $s = 0$) gelten. Nun können wir die ganze Reihe als aus zwei Theilen bestehend ansehen, deren erster die Summe ihrer ersten n Glieder

$$\beta_1\left(\frac{1}{1^s}-\frac{1}{2^s}\right)+\cdots+\beta_n\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right),$$

also eine stetige Function von s ist, während der zweite, wie im Vorhergehenden bewiesen ist, sicher

$$< \frac{C}{n^s} \text{ und also auch } < \frac{C}{n^\sigma}$$

ist; dieser letztere Theil kann also durch die Wahl eines hinreichend grossen Werthes von n, d. h. durch eine zweckmässige Zerlegung der ganzen Reihe, kleiner gemacht werden, als irgend ein vorgeschriebener Werth; und zwar wird, was besonders wichtig ist, für *alle* Werthe von $s > \sigma$ dies durch einen und denselben Werth von n, d. h. durch eine und dieselbe Zerlegung der unendlichen Reihe bewirkt werden. Da nun der erste Bestandtheil stetig ist, so kann eine etwaige Unstetigkeit des Ganzen nur von einer Unstetigkeit des zweiten Bestandtheils herrühren, und folglich muss, da dieser zweite Theil für alle in Betracht kommenden Werthe von s absolut genommen $< Cn^{-\sigma}$ ist, die Grösse einer plötzlichen Werthänderung beim Durchlaufen eines bestimmten Werthes von s jedenfalls $< 2\,Cn^{-\sigma}$ sein. Da wir aber durch zweckmässige Wahl von n diesen Werth beliebig klein machen können, so folgt, dass gar keine Unstetigkeit vorkommen kann; denn fände wirklich ein Sprung um eine Grösse μ Statt, so nehme man n so gross, dass $2\,Cn^{-\sigma} < \mu$ wird, so ergiebt sich augenblicklich der Widerspruch.

Nachdem so der obige Satz vollständig bewiesen ist, wenden wir ihn auf unsere Reihe

$$\Sigma\left(\frac{D}{n}\right)\frac{1}{n^{1+\varrho}}$$

an, in welcher die Glieder von jetzt ab stets *so geordnet* werden sollen, dass die Zahl *n beständig wächst.* Unter *dieser* Voraussetzung erkennt man leicht, dass diese Reihe einen speciellen Fall der in dem vorstehenden Satze untersuchten Reihe bildet; setzt man nämlich

$$\alpha_m = \left(\frac{D}{m}\right) \text{ oder } = 0,$$

je nachdem m relative Primzahl zu $2D$ (also eine Zahl n) ist oder nicht, und lässt m ein vollständiges Restsystem (mod. $4D$) durchlaufen, so ist die Summe der entsprechenden Coefficienten α_m stets $= 0$, weil diese Coefficienten α_m theils selbst $= 0$ sind und die übrigen, wie eine frühere Untersuchung (§. 52) ergeben hat, zur Hälfte den Werth $+1$, zur andern Hälfte den Werth -1 besitzen. Hieraus folgt unmittelbar, dass die Summe von noch so vielen auf einander folgenden Coefficienten α_m stets unterhalb einer endlichen Grösse ($\pm 2D$) bleibt. Mithin ist die in der oben angegebenen Art geordnete Reihe

$$\Sigma \frac{\alpha_m}{m^s} = \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

convergent, so lange s positiv bleibt, und zugleich eine stetige Function von s; und folglich wird, wenn ϱ unendlich klein wird,

$$\lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^{1+\varrho}} = \Sigma \left(\frac{D}{n}\right) \frac{1}{n},$$

wo, wie wir nochmals hervorheben, die Glieder der Reihe *so geordnet* sind, dass *n beständig wächst.*

§. 102.

Es ist nun zweckmässig, bei der Bestimmung der Summe der unendlichen Reihe

$$N = \Sigma \left(\frac{D}{n}\right) \frac{1}{n}$$

dieselben vier Fälle zu unterscheiden, welche wir früher (§. 52) aufgestellt haben. Wir wenden uns zunächst zu dem Fall, in welchem

$$D = \pm P \equiv 1 \text{ (mod. 4), also } \left(\frac{D}{n}\right) = \left(\frac{n}{P}\right)$$

ist, wo P den absoluten Werth von D bedeutet, und also eine positive ungerade, durch kein Quadrat theilbare Zahl und > 1 ist. Dann lässt sich die Reihe

$$N = \Sigma \left(\frac{n}{P}\right) \frac{1}{n}$$

leicht auf die Reihe

$$M = \Sigma \left(\frac{m}{P}\right)\frac{1}{m}$$

zurückführen, in welcher m beständig wachsend *alle* positiven relativen Primzahlen zu P, auch die *geraden* durchläuft. Da jedesmal, wenn m ein vollständiges Restsystem (mod. P) durchläuft, zufolge §. 52, (3)

$$\Sigma \left(\frac{m}{P}\right) = 0$$

ist, so convergirt die Reihe M; ist ferner k eine beliebige positive ganze Zahl, und betrachtet man alle diejenigen Zahlen m, welche $< 2kP$ sind, so sind dieselben zum Theil ungerade, zum Theil gerade; die erstern stimmen offenbar mit allen Zahlen $n < 2kP$ überein, und die letztern sind von der Form $2m'$, wo m' alle diejenigen Zahlen m durchläuft, welche $< kP$ sind. In dieser Ausdehnung ist daher

$$\Sigma \left(\frac{m}{P}\right)\frac{1}{m} = \Sigma \left(\frac{n}{P}\right)\frac{1}{n} + \Sigma \left(\frac{2m'}{P}\right)\frac{1}{2m'}$$
$$= \Sigma \left(\frac{n}{P}\right)\frac{1}{n} + \left(\frac{2}{P}\right)\frac{1}{2}\,\Sigma \left(\frac{m'}{P}\right)\frac{1}{m'},$$

und hieraus folgt, wenn man k über alle Grenzen wachsen lässt,

$$M = N + \left(\frac{2}{P}\right)\frac{1}{2}\cdot M,\quad N = \left(1 - \left(\frac{2}{P}\right)\frac{1}{2}\right)M.$$

Allgemeiner findet man leicht, dass

$$\Sigma \left(\frac{n}{P}\right)\frac{1}{n^s} = \left(1 - \left(\frac{2}{P}\right)\frac{1}{2^s}\right)\Sigma \left(\frac{m}{P}\right)\frac{1}{m^s}$$

ist; man braucht nur den reciproken Werth des ersten Factors auf der rechten Seite in eine geometrische Reihe zu verwandeln, und diese mit der Reihe auf der linken Seite zu multipliciren, so ergiebt sich als Product der zweite Factor auf der rechten Seite; oder man kann auch genau so wie oben verfahren, indem man die Zahlen m zerlegt in die Zahlen n und $2m'$.

§. 103.

Die nun noch auszuführende Summation kann mit Hülfe des in den Supplementen (I. §. 116) bewiesenen Satzes auf verschiedene Arten bewerkstelligt werden, entweder durch Zurückführung auf Fourier'sche Reihen, oder durch die Integration eines rationalen Bruchs. Wir schlagen den letztern Weg als den directern ein. Bedeutet m irgend eine positive ganze Zahl, so ist bekanntlich

$$\frac{1}{m} = \int_0^1 x^{m-1}\,dx,$$

und folglich ist auch

$$M = \Sigma\left(\frac{m}{P}\right)\frac{1}{m} = \Sigma\left(\frac{m}{P}\right)\int_0^1 x^{m-1}\,dx.$$

Da nun das Jacobi'sche Symbol für alle einander nach dem Modul P congruenten Zahlen m denselben Werth hat, so ist die Summe der Glieder unserer Reihe, in welchen $m < kP$, gleich

$$\int_0^1 \frac{dx}{x} f(x)\,\frac{1-x^{kP}}{1-x^P},$$

wo zur Abkürzung

$$f(x) = \Sigma\left(\frac{\mu}{P}\right) x^\mu$$

gesetzt ist, und der Summationsbuchstabe μ die Werthe m durchlaufen muss, welche $< P$ sind. Da dieselben ein vollständiges Restsystem in Bezug auf den Modul P bilden, so ist nach einem schon öfter benutzten Satze (§. 52)

$$f(1) = \Sigma\left(\frac{\mu}{P}\right) = 0;$$

es ist folglich $f(x)$ theilbar durch $x(x-1)$, und mithin hat der Bruch

$$\frac{1}{x}\cdot\frac{f(x)}{1-x^P}$$

im reellen Integrationsintervall $0 \leqq x \leqq 1$ endliche Werthe. Hieraus folgt leicht, dass mit unbegrenzt wachsendem k das Integral

$$\int_0^1 \frac{dx}{x} \frac{f(x)\, x^{kP}}{1-x^P}$$

unendlich klein wird, und wir erhalten folglich

$$\Sigma \left(\frac{m}{P}\right) \frac{1}{m} = \int_0^1 \frac{dx}{x} \frac{f(x)}{1-x^P};$$

die Aufgabe ist mithin darauf zurückgeführt, einen echten rationalen Bruch zu integriren, was bekanntlich durch Zerlegung desselben in sogenannte Partialbrüche geschieht. Setzen wir zur Abkürzung

$$\sqrt{-1} = i, \quad e^{\frac{2\pi i}{P}} = \theta,$$

so ist in unserm Fall der Nenner

$$x^P - 1 = \Pi(x - \theta^\alpha),$$

wo das Productzeichen sich auf den Buchstaben α bezieht, welcher ein vollständiges Restsystem in Bezug auf den Modul P durchlaufen muss; wir setzen fest, dass α die Werthe

$$0, 1, 2 \ldots (P-1)$$

durchlaufen soll; man erhält dann nach bekannten Regeln

$$\frac{1}{x} \frac{f(x)}{1-x^P} = -\frac{1}{P} \Sigma \frac{f(\theta^\alpha)}{x-\theta^\alpha},$$

wo das Summenzeichen sich auf den Buchstaben α bezieht. Nach der oben eingeführten Bezeichnung ist nun

$$f(\theta^\alpha) = \Sigma \left(\frac{\mu}{P}\right) e^{\mu \frac{2\alpha\pi i}{P}},$$

und diese Summe ist vermöge des in den Supplementen (I. §. 116) bewiesenen Satzes

$$= \left(\frac{\alpha}{P}\right) \sqrt{P} \,.\, i^{1/4(P-1)^2}$$

wo die Quadratwurzel $\sqrt{P}$ *positiv*, und

$$\left(\frac{\alpha}{P}\right) = 0$$

zu nehmen ist, wenn α keine relative Primzahl zu P ist. Die Zerlegung in Partialbrüche liefert uns also das Resultat

$$\frac{1}{x} \frac{f(x)}{1-x^P} = -\frac{i^{1/4(P-1)^2}}{\sqrt{P}} \Sigma \frac{\left(\frac{\alpha}{P}\right)}{x-\theta^\alpha},$$

wo das Summenzeichen sich auf den Buchstaben α bezieht, der nur alle die positiven ganzen Zahlen zu durchlaufen braucht, welche $< P$ und relative Primzahlen zu P sind.

Die nun auszuführenden Integrationen der einzelnen $\varphi(P)$ Partialbrüche sind in der einen Formel

$$\int \frac{dx}{x-a-bi} = \tfrac{1}{2}\log\left\{(x-a)^2+b^2\right\} + i\,\mathrm{arctang}\frac{x-a}{b}$$

oder

$$\int \frac{dx}{x-e^{\delta i}} = \tfrac{1}{2}\log\left\{x^2-2x\cos\delta+1\right\} + i\,\mathrm{arctang}\frac{x-\cos\delta}{\sin\delta}$$

enthalten, aus welcher, wenn $0 < \delta < 2\pi$ ist,

$$\int_0^1 \frac{dx}{x-e^{\delta i}} =$$

$$\log(2\sin\tfrac{1}{2}\delta) + i\left\{\mathrm{arctang}(\mathrm{tang}\,\tfrac{1}{2}\delta) + \mathrm{arctang}(\mathrm{cotang}\,\delta)\right\}$$

folgt, vorausgesetzt, dass die beiden Arcus, welche in der Parenthese stehen, in dem Intervall zwischen $+\frac{1}{2}\pi$ und $-\frac{1}{2}\pi$ genommen werden. Mag nun δ zwischen 0 und π, oder zwischen π und 2π liegen, so ergiebt sich hieraus leicht, dass immer

$$\int_0^1 \frac{dx}{x-e^{\delta i}} = \log(2\sin\tfrac{1}{2}\delta) + i(\tfrac{1}{2}\pi - \tfrac{1}{2}\delta)$$

ist.

Wenden wir dies auf unsern Fall an, so erhalten wir

$$\int_0^1 \frac{dx}{x-\theta^\alpha} = \log\left(2\sin\frac{\alpha\pi}{P}\right) + i\left(\frac{\pi}{2}-\frac{\alpha\pi}{P}\right)$$

und folglich

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m} = -\frac{i^{1/4(P-1)^2}}{\sqrt{P}}\,\Sigma\left(\frac{\alpha}{P}\right)\left\{\log\left(2\sin\frac{\alpha\pi}{P}\right) + i\left(\frac{\pi}{2}-\frac{\alpha\pi}{P}\right)\right\},$$

wo das Summenzeichen rechts sich auf alle $\varphi(P)$ Werthe von α erstreckt. Da nun

$$\Sigma\left(\frac{\alpha}{P}\right) = 0$$

ist, so können die in der Parenthese befindlichen Glieder, welche von α unabhängig sind, wie log 2 und $\frac{1}{2}\pi i$ weggelassen werden, und man erhält dann

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m}=-\frac{i^{1/4(P-1)^2}}{\sqrt{P}}\,\Sigma\left(\frac{\alpha}{P}\right)\left\{\log\sin\frac{\alpha\pi}{P}-\frac{\alpha\pi i}{P}\right\}.$$

Dieses Resultat nimmt noch einfachere Formen an, wenn man die beiden Fälle $P\equiv 1 \pmod 4$ und $P\equiv 3 \pmod 4$ von einander trennt. Im erstern Falle ist nämlich

$$i^{1/4(P-1)^2}=1$$

und folglich, da die linke Seite reell ist,

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m}=-\frac{1}{\sqrt{P}}\,\Sigma\left(\frac{\alpha}{P}\right)\log\sin\frac{\alpha\pi}{P}$$

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha=0;$$

im letztern Fall dagegen ist

$$i^{1/4(P-1)^2}=i$$

und folglich

$$\Sigma\left(\frac{m}{P}\right)\frac{1}{m}=-\frac{\pi}{P\sqrt{P}}\,\Sigma\left(\frac{\alpha}{P}\right)\alpha$$

$$\Sigma\left(\frac{\alpha}{P}\right)\log\sin\frac{\alpha\pi}{P}=0.$$

Diese beiden Vereinfachungen lassen sich auch auf folgende Weise verificiren. Bedenkt man, dass $(P-\alpha)$ dieselben Werthe wie α durchläuft, so folgt

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha=\Sigma\left(\frac{P-\alpha}{P}\right)(P-\alpha)=-\Sigma\left(\frac{-\alpha}{P}\right)\alpha$$

$$\Sigma\left(\frac{\alpha}{P}\right)\log\sin\frac{\alpha\pi}{P}=\Sigma\left(\frac{P-\alpha}{P}\right)\log\sin\frac{(P-\alpha)\pi}{P}$$

$$=\Sigma\left(\frac{-\alpha}{P}\right)\log\sin\frac{\alpha\pi}{P};$$

ist nun $P\equiv 1 \pmod 4$, so folgt hieraus

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha=-\Sigma\left(\frac{\alpha}{P}\right)\alpha=0;$$

ist dagegen $P\equiv 3 \pmod 4$, so ergiebt sich

$$\Sigma\left(\frac{\alpha}{P}\right)\log\sin\frac{\alpha\pi}{P}=-\Sigma\left(\frac{\alpha}{P}\right)\log\sin\frac{\alpha\pi}{P}=0.$$

§. 104.

Hiermit ist nun für den von uns betrachteten Fall, in welchem die Determinante $D = \pm P \equiv 1 \pmod{4}$ und durch kein Quadrat theilbar ist, der gesuchte Grenzwerth

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = \left(1 - \left(\frac{2}{P}\right) \frac{1}{2}\right) \Sigma \left(\frac{m}{P}\right) \frac{1}{m}$$

wirklich in Form eines geschlossenen Ausdrucks gefunden, und um die Anzahl h der zu dieser Determinante D gehörenden ursprünglichen Formen der ersten Art zu erhalten, brauchen wir nur noch die beiden Fälle, in welchen D negativ oder positiv ist, von einander zu trennen.

Erstens. Ist D negativ $= - P$, und also $P \equiv 3 \pmod{4}$, so ist (§. 97)

$$h = \frac{2\sqrt{-D}}{\pi} \Sigma \left(\frac{D}{n}\right) \frac{1}{n}$$

und da in diesem Fall

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = \left(1 - \left(\frac{2}{P}\right) \frac{1}{2}\right) \Sigma \left(\frac{m}{P}\right) \frac{1}{m}$$

$$= - \left(1 - \left(\frac{2}{P}\right) \frac{1}{2}\right) \frac{\pi}{P\sqrt{P}} \Sigma \left(\frac{\alpha}{P}\right) \alpha$$

ist, so ergiebt sich

$$h = - \frac{1}{P} \left(2 - \left(\frac{2}{P}\right)\right) \Sigma \left(\frac{\alpha}{P}\right) \alpha,$$

wo α wieder alle positiven ganzen Zahlen durchlaufen muss, die $< P$ und relative Primzahlen zu P sind. Offenbar muss dieser Ausdruck für die Classenanzahl sich noch in der Weise umformen lassen, dass der Divisor P verschwindet. Dies lässt sich in der That durch folgende Betrachtung erreichen. Bezeichnet man mit α' diejenigen Zahlen α, welche $< \frac{1}{2} P$ sind, so stimmen die Zahlen $(P - \alpha')$ mit denjenigen Zahlen α überein, welche $> \frac{1}{2} P$ sind; es ist daher

$$\Sigma \left(\frac{\alpha}{P}\right) \alpha = \Sigma \left(\frac{\alpha'}{P}\right) \alpha' + \Sigma \left(\frac{P - \alpha'}{P}\right) (P - \alpha'),$$

wo die Summenzeichen rechts sich auf den Buchstaben α' beziehen; da nun $P \equiv 3 \pmod{4}$, und also

$$\left(\frac{P-\alpha'}{P}\right)=\left(\frac{-1}{P}\right)\left(\frac{\alpha'}{P}\right)=-\left(\frac{\alpha'}{P}\right)$$

ist, so erhalten wir

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha=2\,\Sigma\left(\frac{\alpha'}{P}\right)\alpha'-P\,\Sigma\left(\frac{\alpha'}{P}\right).$$

Offenbar wird die Reihe aller Zahlen α aber auch erschöpft durch die sämmtlichen Zahlen $2\alpha'$ und $(P-2\alpha')$, und folglich ist auch

$$\Sigma\left(\frac{\alpha}{P}\right)\alpha=\Sigma\left(\frac{2\alpha'}{P}\right)2\alpha'+\Sigma\left(\frac{P-2\alpha'}{P}\right)(P-2\alpha')$$

oder nach leichten Reductionen

$$\left(\frac{2}{P}\right)\Sigma\left(\frac{\alpha}{P}\right)\alpha=4\,\Sigma\left(\frac{\alpha'}{P}\right)\alpha'-P\,\Sigma\left(\frac{\alpha'}{P}\right).$$

Zieht man diese Gleichung von der frühern ab, nachdem dieselbe mit 2 multiplicirt ist, so erhält man

$$\left\{2-\left(\frac{2}{P}\right)\right\}\Sigma\left(\frac{\alpha}{P}\right)\alpha=-P\,\Sigma\left(\frac{\alpha'}{P}\right)$$

und hierdurch verwandelt sich der obige Ausdruck für die Classenanzahl in den folgenden einfachsten:

$$h=\Sigma\left(\frac{\alpha'}{P}\right).$$

Wir können daher für diesen Fall als Resultat unserer ganzen Untersuchung folgenden Satz aussprechen:

Ist P eine positive, durch kein Quadrat theilbare Zahl von der Form $4n+3$, und bezeichnet man mit α' alle relativen Primzahlen zu P, welche $<\frac{1}{2}P$ sind, so findet man die Classenanzahl h der zu der Determinante $D=-P$ gehörenden Formen der ersten Art, wenn man von der Anzahl derjenigen der Zahlen α', für welche

$$\left(\frac{\alpha'}{P}\right)=+1$$

ist, die Anzahl der übrigen Zahlen α' abzieht.

Der Ausdruck dieses Satzes vereinfacht sich in dem speciellen Fall, wenn P eine einfache Primzahl ist, folgendermaassen:

Ist der absolute Werth p der negativen Determinante $D=-p$ eine Primzahl von der Form $4n+3$, so ist die Classenanzahl h der zu ihr gehörigen Formen der ersten Art gleich dem Ueberschuss der Anzahl der zwischen 0 und $\frac{1}{2}p$ liegenden quadratischen Reste

von p über die Anzahl der zwischen denselben Grenzen liegenden quadratischen Nichtreste von p.

Dieser letztere Satz ist in einer nicht wesentlich verschiedenen Form schon einige Zeit vor der Veröffentlichung der Lösung des allgemeinen Problems*) durch Induction von *Jacobi***) gefunden.

Als Beispiel wählen wir die Determinante $D = -11$; unter den Zahlen 1, 2, 3, 4, 5 sind vier quadratische Reste 1, 3, 4, 5, und ein quadratischer Nichtrest 2 von 11; mithin ist die Anzahl der Formen erster Art $= 4 - 1 = 3$. In der That giebt es für diese Determinante nur drei (nicht äquivalente) reducirte Formen erster Art, nämlich (1, 0, 11), (3, 1, 4) und (3, − 1, 4).

Beiläufig mag hier bemerkt werden, dass zufolge des gewonnenen Resultats die Anzahl der Zahlen α', für welche

$$\left(\frac{\alpha'}{P}\right) = +1,$$

stets grösser ist, als die Anzahl der Zahlen α', für welche

$$\left(\frac{\alpha'}{P}\right) = -1$$

ist, da h immer eine positive Zahl, nie $= 0$ ist: ein Satz, welcher auch für den einfachsten Fall, wo P eine Primzahl von der Form $4n + 3$ ist, auf anderm Wege noch nicht hat bewiesen werden können (vergl. das Theorem über die arithmetische Progression, Supplement VI.).

Zweitens. Ist die Determinante D positiv $= +P$, und also $P \equiv 1 \pmod{4}$, so ist (nach §. 99) die Classenanzahl

$$h = \frac{2\sqrt{D}}{\log(T + U\sqrt{D})} \, \Sigma \left(\frac{D}{n}\right) \frac{1}{n}$$

und da in diesem Fall

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n} = \left(1 - \left(\frac{2}{P}\right) \frac{1}{2}\right) \Sigma \left(\frac{m}{P}\right) \frac{1}{m}$$

---

*) *Dirichlet: Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres* in Crelle's Journal XIX und XXI.

**) *Observatio arithmetica* in Crelle's Journal IX; vergl. *Dirichlet: Gedächtnissrede auf C. G. J. Jacobi,* und *Kummer: Gedächtnissrede auf G. P. Lejeune Dirichlet.*

$$= -\frac{1-\left(\frac{2}{P}\right)\frac{1}{2}}{\sqrt{P}} \Sigma \left(\frac{\alpha}{P}\right) \log \sin \frac{\alpha\pi}{P}$$

ist, so ergiebt sich

$$h = -\frac{2-\left(\frac{2}{P}\right)}{\log(T+U\sqrt{P})} \Sigma \left(\frac{\alpha}{P}\right) \log \sin \frac{\alpha\pi}{P}.$$

Bezeichnet man die Zahlen α mit a oder mit b, je nachdem

$$\left(\frac{\alpha}{P}\right) = +1 \text{ oder } = -1$$

ist, so nimmt die vorstehende Gleichung folgende Gestalt an:

$$h = \frac{2-\left(\frac{2}{P}\right)}{\log(T+U\sqrt{P})} \log \frac{\Pi \sin \frac{b\pi}{P}}{\Pi \sin \frac{a\pi}{P}};$$

hierin beziehen sich die Productzeichen Π im Zähler und Nenner resp. auf alle b und auf alle a; und ausserdem bedeuten T, U die kleinsten positiven ganzen Zahlen, welche der Pell'schen Gleichung

$$T^2 - PU^2 = 1$$

genügen. Der wahre Charakter dieses Resultates wird durch eine weitere Umformung (§. 107) noch deutlicher werden.

§. 105.

Nachdem im Vorhergehenden (§§. 102 bis 104) der Fall, in welchem $D \equiv 1 \pmod{4}$ ist, seine vollständige Erledigung gefunden hat, begnügen wir uns, die Hauptmomente für die allgemeine Untersuchung hervorzuheben. Es handelt sich zunächst um die Bestimmung der Reihe

$$N = \Sigma \left(\frac{D}{n}\right) \frac{1}{n},$$

in welcher n beständig wachsend alle positiven ganzen Zahlen durchlaufen muss, die relative Primzahlen zu $2D$ sind.

Gebrauchen wir nun die Buchstaben P, δ, ε genau in derselben Bedeutung, wie sie am Schluss des §. 52 festgesetzt ist, so ist

$$\left(\frac{D}{n}\right) = \delta^{\frac{1}{2}(n-1)}\,\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{P}\right),$$

und folglich stets

$$\left(\frac{D}{n}\right) = \left(\frac{D}{\nu}\right),$$

wenn $n \equiv \nu \pmod{8P}$ ist. Setzt man daher

$$\frac{1}{n} = \int_0^1 x^{n-1}\,dx,$$

und

$$f(x) = \Sigma \left(\frac{D}{\nu}\right) x^{\nu},$$

wo ν alle die Zahlen n durchläuft, welche $< 8P$ sind, und berücksichtigt, dass $f(1) = 0$ ist (§. 52), so findet man unter der Voraussetzung, dass der Modulus von x auf dem Integrationswege < 1 bleibt, ähnlich wie in §. 103,

$$N = \int_0^1 \frac{f(x)}{1 - x^{8P}}\,\frac{dx}{x} = -\frac{1}{8P}\int_0^1 \Sigma\,\frac{f(\omega)\,dx}{x - \omega},$$

wo ω alle Wurzeln der Gleichung

$$\omega^{8P} = 1$$

durchlaufen muss; diese sind bekanntlich von der Form

$$\omega = j^r \theta^s,$$

wo zur Abkürzung

$$j = e^{\frac{\pi i}{4}} = \frac{1+i}{\sqrt{2}},\quad \theta = e^{\frac{2\pi i}{P}}$$

gesetzt ist; lässt man r und s vollständige Restsysteme resp. nach den Moduln 8 und P durchlaufen, so erhält ω seine sämmtlichen $8P$ Werthe.

Bedeuten nun μ und m resp. die kleinsten positiven Reste der Zahl ν in Bezug auf die Moduln 8 und P, so ist μ eine der vier Zahlen 1, 3, 5, 7, und m eine der $\varphi(P)$ relativen Primzahlen zu P; und da umgekehrt jedem solchen Restpaare μ, m eine und nur eine bestimmte Zahl ν entspricht (§. 25), so findet man, mit Zuziehung des in den Supplementen (§. 116) bewiesenen Hülfssatzes,

$$f(\omega) = \Sigma \left(\frac{D}{\nu}\right) \omega^{\nu} = \Sigma\, \delta^{1/2(\nu-1)}\, \varepsilon^{1/8(\nu^2-1)} \left(\frac{\nu}{P}\right) j^{\nu r} \theta^{\nu s}$$

$$= \Sigma\, \delta^{1/2(\mu-1)}\, \varepsilon^{1/8(\mu^2-1)} j^{\mu r}\, \Sigma \left(\frac{m}{P}\right) \theta^{ms}$$

$$= j^r (1 + \delta i^{3r}) (1 + \varepsilon (-1)^r) \left(\frac{s}{P}\right) i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P},$$

wo $\sqrt{P}$ *positiv* ist, und das Jacobi'sche Symbol den Werth Null hat, wenn s keine relative Primzahl zu P ist. Wenn $P = 1$, so sind die Factoren, in welchen P vorkommt wegzulassen. Setzen wir nun zur Abkürzung

$$\psi(r) = \int_0^1 \Sigma \left(\frac{s}{P}\right) \frac{dx}{x - j^r \theta^s},$$

wo s alle incongruenten Zahlen (mod. P) zu durchlaufen hat, die relative Primzahlen zu P sind, so ergiebt sich

$$N = -\frac{i^{\left(\frac{P-1}{2}\right)^2}}{8\sqrt{P}} \Sigma\, j^r (1 + \delta i^{3r}) (1 + \varepsilon (-1)^r) \psi(r),$$

wo r ein vollständiges Restsystem (mod. 8) durchlaufen muss. Trennt man jetzt die vier Fälle von einander, so erhält man folgende Resultate:

I. $D = \pm P \equiv 1$ (mod. 4), $\delta = +1$, $\varepsilon = +1$;

$$N \,.\, 2\sqrt{P} = -i^{\left(\frac{P-1}{2}\right)^2} \{\psi(0) - \psi(4)\}.$$

II. $D = \pm P \equiv 3$ (mod. 4), $\delta = -1$, $\varepsilon = +1$;

$$N \,.\, 2\sqrt{P} = -i \,.\, i^{\left(\frac{P-1}{2}\right)^2} \{\psi(2) - \psi(6)\}.$$

III. $D = \pm 2P \equiv 2$ (mod. 8), $\delta = +1$, $\varepsilon = -1$;

$$N \,.\, 2\sqrt{2P} = -i^{\left(\frac{P-1}{2}\right)^2} \{\psi(1) - \psi(3) - \psi(5) + \psi(7)\}.$$

IV. $D = \pm 2P \equiv 6$ (mod. 8), $\delta = -1$, $\varepsilon = -1$;

$$N \,.\, 2\sqrt{2P} = -i \,.\, i^{\left(\frac{P-1}{2}\right)^2} \{\psi(1) + \psi(3) - \psi(5) - \psi(7)\}.$$

Dieselben Formeln gelten auch noch für den Fall $P = 1$, d. h. für die Fälle $D = -1$, $D = +2$, $D = -2$, wenn

$$\psi(r) = \int_0^1 \frac{dx}{x - j^r}$$

gesetzt wird. Zur Bestimmung der Werthe $\psi(r)$, auf welche es jetzt allein noch ankommt, dient wieder die unter der Voraussetzung $0 < \varphi < 2\pi$ gültige Gleichung

$$\int_0^1 \frac{dx}{x - e^{\varphi i}} = \log(2 \sin \tfrac{1}{2}\varphi) + \tfrac{1}{2}(\pi - \varphi) i,$$

und man findet hieraus für den Fall $P = 1$ leicht folgende Resultate:

$$\begin{aligned} D &= -1; \quad N = \frac{\pi}{4} \\ D &= +2; \quad N = \frac{\log(1 + \sqrt{2})}{\sqrt{2}} \\ D &= -2; \quad N = \frac{\pi}{2\sqrt{2}}, \end{aligned} \qquad (1)$$

wo $\sqrt{2}$ positiv zu nehmen ist. Schliessen wir von jetzt an den Fall $P = 1$ gänzlich aus, so ist

$$\int_0^1 \frac{dx}{x - j^r \theta^s} = \log\left(2 \sin \frac{m\pi}{8P}\right) + \left(\frac{\pi}{2} - \frac{m\pi}{8P}\right) i,$$

wo m den kleinsten positiven Rest der Zahl $(Pr + 8s)$ nach dem Modul $8P$ bedeutet, so dass

$$m \equiv Pr \pmod{8}, \; m \equiv 8s \pmod{P}, \; 0 < m < 8P$$

ist; hieraus folgt

$$\psi(r) = \left(\frac{2}{P}\right) \Sigma \left(\frac{m}{P}\right) \left\{\log\left(2 \sin \frac{m\pi}{8P}\right) + \left(\frac{\pi}{2} - \frac{m\pi}{8P}\right) i\right\},$$

wo m diejenigen $\varphi(P)$ positiven Zahlen durchlaufen muss, welche relative Primzahlen zu P, kleiner als $8P$ und zugleich $\equiv Pr \pmod{8}$ sind; da dieselben nach dem Modul P incongruent sind, so ist (§. 52)

$$\Sigma \left(\frac{m}{P}\right) = 0,$$

und folglich nimmt die vorstehende Gleichung folgende einfachere Gestalt an

$$\begin{aligned} \psi(r) &= \left(\frac{2}{P}\right) \Sigma \left(\frac{m}{P}\right) \left(\log \sin \frac{m\pi}{8P} - \frac{m\pi i}{8P}\right), \\ m &\equiv Pr \pmod{8}, \quad 0 < m < 8P. \end{aligned} \qquad (2)$$

Hierdurch ist nun der Werth der unendlichen Reihe N in allen Fällen auf eine Summe von einer endlichen Anzahl von Glie-

dern zurückgeführt; dieselbe ist aber noch bedeutender Vereinfachungen fähig, zufolge gewisser Eigenschaften der acht Ausdrücke $\psi(r)$, die entweder aus der so eben gefundenen Form, oder auch aus ihrer ursprünglichen Definition leicht abgeleitet werden können. Indem wir den letztern Weg einschlagen, setzen wir zur Abkürzung

$$F(x) = \Pi\,(x-\theta^s)^{\left(\frac{s}{P}\right)} = \frac{\Pi\,(x-\theta^a)}{\Pi\,(x-\theta^b)} \tag{3}$$

wo die Buchstaben a und b die in §. 52 festgesetzte Bedeutung haben; dann wird zufolge der obigen Definition

$$\psi(r) = \int_0^1 d \log F(xj^{-r}),$$

wo der Modulus der Variabeln x auf dem Wege von 0 bis 1 stets < 1 bleibt, oder auch

$$\psi(r) = \int_0^{j^{-r}} d \log F(x),$$

wo, wenn die complexen Grössen in der bekannten Weise geometrisch durch Puncte einer Ebene dargestellt werden, der Punct x von 0 bis j^{-r} sich so bewegen muss, dass er im Innern des mit dem Halbmesser 1 um den Punct 0 beschriebenen Kreises bleibt. Die acht Puncte j^r zerlegen die Peripherie dieses Kreises in acht gleiche Octanten, auf welche sich die $\varphi(P)$ Puncte θ^s vertheilen, die ihrerseits wieder in zwei Classen θ^a und θ^b zerfallen.

Aus der Definition der Function $F(x)$ geht zunächst hervor, dass sie mit

$$\Pi\,(x'-\theta^{-s})^{\left(\frac{s}{P}\right)} = F(x')^{\left(\frac{-1}{P}\right)}$$

conjugirt ist, wenn x' den mit x conjugirten complexen Werth bedeutet; und hieraus folgt unmittelbar, dass $\psi(r)$ und

$$\left(\frac{-1}{P}\right)\int_0^{j^r} d \log F(x') = \left(\frac{-1}{P}\right)\psi(-r)$$

ebenfalls conjugirt sind. Setzt man daher zur Abkürzung

$$\left.\begin{aligned} R(r) &= \psi(-r) + \left(\frac{-1}{P}\right)\psi(r), \\ J(r) &= \psi(-r) - \left(\frac{-1}{P}\right)\psi(r), \end{aligned}\right\} \tag{4}$$

so wird R reell, und J rein imaginär oder $= 0$; und man erkennt leicht, dass die Summe N sich auf Ausdrücke von der Form R oder J reducirt, je nachdem die Determinante D positiv oder negativ ist.

Aus der Definition der Function $F(x)$ folgt ferner leicht die Relation

$$F(x)\,F(-x) = F(x^2)^{\left(\frac{2}{P}\right)}; \tag{5}$$

da nun, wenn x im Innern des Kreises von 0 bis j^{-r} geht, gleichzeitig $-x$ von 0 bis $j^{-(r+4)}$, und x^2 von 0 bis j^{-2r} fortrückt, so ergiebt sich

$$\psi(r) + \psi(r+4) = \left(\frac{2}{P}\right)\psi(2r); \tag{6}$$

dieselbe Eigenschaft kommt offenbar auch den Ausdrücken R und J zu.

Die Function $F(x)$ besitzt endlich noch die folgende Eigenschaft

$$F\left(\frac{1}{x}\right) = \theta^{\Sigma\left(\frac{s}{P}\right)s}\,F(x)^{\left(\frac{-1}{P}\right)}; \tag{7}$$

da nun, wenn x im Innern des Kreises von 0 bis j^{-r} geht, der reciproke Werth y ausserhalb des Kreises von ∞ bis j^r fortrückt, so folgt

$$\int_{\infty}^{j^r} d\log F(y) = \left(\frac{-1}{P}\right)\psi(r),$$

und hieraus ergiebt sich

$$J(r) = \int_0^{\infty} d\log F(z_r),$$

wo z_r im Innern des Kreises von 0 bis j^r, dann ausserhalb desselben von j^r bis ∞ geht. Die Differenz $J(r) - J(r+1)$ ist daher ein geschlossenes Integral, in welchem die Integrationsvariabele einen positiven Umlauf um diejenigen Puncte θ^s macht, die auf dem von den Puncten j^r und j^{r+1} begrenzten Octanten liegen, und folglich ist nach bekannten Sätzen der complexen Integration

$$J(r) - J(r+1) = 2\pi i \sum_r^{r+1}\left(\frac{s}{P}\right),$$

wo s alle Werthe durchläuft, die der Bedingung

$$\frac{r}{8} < \frac{s}{P} < \frac{r+1}{8}$$

genügen; hieraus ergiebt sich weiter

$$J(r) - J(r+4) = 2\pi i \sum_{r}^{r+4} \left(\frac{s}{P}\right),$$

und ebenso, wenn r *positiv* ist,

$$J(r) - J(2r) = 2\pi i \sum_{r}^{2r} \left(\frac{s}{P}\right);$$

setzt man die hieraus folgenden Werthe von $J(r+4)$ und $J(2r)$ in die aus (6) abgeleitete Gleichung

$$J(r) + J(r+4) = \left(\frac{2}{P}\right) J(2r)$$

ein, so erhält man

$$\left\{2 - \left(\frac{2}{P}\right)\right\} J(r) = 2\pi i \left\{\sum_{r}^{r+4} \left(\frac{s}{P}\right) - \left(\frac{2}{P}\right) \sum_{r}^{2r} \left(\frac{s}{P}\right)\right\}.$$

Bedenkt man ferner, dass

$$\sum_{4}^{4+r} \left(\frac{s}{P}\right) = \left(\frac{-1}{P}\right) \sum_{4-r}^{4} \left(\frac{s}{P}\right)$$

ist, so ergiebt sich

$$\left\{2 - \left(\frac{2}{P}\right)\right\} J(0) = 2\pi i \sum_{0}^{4} \left(\frac{s}{P}\right)$$

$$\left\{2 - \left(\frac{2}{P}\right)\right\} J(2) = 2\pi i \left\{1 + \left(\frac{-1}{P}\right) - \left(\frac{2}{P}\right)\right\} \sum_{2}^{4} \left(\frac{s}{P}\right)$$

$$J(1) + \left(\frac{-1}{P}\right) J(3) = 2\pi i \left\{\sum_{1}^{4} \left(\frac{s}{P}\right) + \left(\frac{-1}{P}\right) \sum_{3}^{4} \left(\frac{s}{P}\right)\right\}.$$

Da endlich zufolge (6) und (4)

$$\psi(0) - \psi(4) = \left\{2 - \left(\frac{2}{P}\right)\right\} \psi(0),$$

$$\left\{1 - \left(\frac{-1}{P}\right)\right\} \psi(0) = J(0),$$

$$\psi(6) - \left(\frac{-1}{P}\right) \psi(2) = J(2),$$

$$\{\psi(7) - \psi(3)\} + \left(\frac{-1}{P}\right) \{\psi(5) - \psi(3)\} = J(1) + \left(\frac{-1}{P}\right) J(3)$$

ist, so wird, wenn die Determinante D *negativ*, also P im ersten und dritten Falle $\equiv 3$, im zweiten und vierten Falle $\equiv 1 \pmod{4}$ ist,

$$\text{I.}\quad N = \frac{\pi}{2\sqrt{P}} \sum_0^4 \left(\frac{s}{P}\right),$$

$$\text{II.}\quad N = \frac{\pi}{\sqrt{P}} \sum_0^2 \left(\frac{s}{P}\right),$$

$$\text{III.}\quad N = \frac{\pi}{\sqrt{2P}} \sum_1^3 \left(\frac{s}{P}\right),$$

$$\text{IV.}\quad N = \frac{\pi}{\sqrt{2P}} \left\{\sum_0^1 \left(\frac{s}{P}\right) - \sum_3^4 \left(\frac{s}{P}\right)\right\},$$

wenn man berücksichtigt, dass im zweiten und vierten Falle

$$\sum_0^4 \left(\frac{s}{P}\right) = 0$$

ist.

Für *positive* Determinanten erhält man ebenfalls Vereinfachungen durch die Betrachtung des *reellen* Ausdrucks (4)

$$R(r) = \int_0^1 \Sigma \left(\frac{s}{P}\right) \left\{\frac{dx}{x - j^{-r}\theta^s} + \frac{dx}{x - j^r\theta^{-s}}\right\}$$

$$= \Sigma \left(\frac{s}{P}\right) \log\{(j^r - \theta^s)(j^{-r} - \theta^{-s})\}$$

$$= \log\{F(j^r)F(j^{-r})^{\left(\frac{-1}{P}\right)}\},$$

welcher zufolge (7) in den folgenden übergeht

$$R(r) = \log\{cF(j^r)^2\},$$

wo

$$c = \theta^{\Sigma b - \Sigma a} = \frac{-1 + i\sqrt{3}}{2} \quad \text{oder} \quad = 1$$

ist, je nachdem $P = 3$ oder von 3 verschieden ist (§. 140). Da nun zufolge (6) und (4)

$$\psi(0) - \psi(4) = \left\{2 - \left(\frac{2}{P}\right)\right\} \psi(0)$$

$$\left\{1 + \left(\frac{-1}{P}\right)\right\} \psi(0) = R(0)$$

$$\psi(6) + \left(\frac{-1}{P}\right) \psi(2) = R(2)$$

$$\psi(7) + \left(\frac{-1}{P}\right) \psi(1) = R(1)$$

$$\psi(5) + \left(\frac{-1}{P}\right) \psi(3) = R(3)$$

ist, so erhält man, weil im ersten und dritten Falle $P \equiv 1$, im zweiten und vierten Falle $P \equiv 3 \pmod{4}$ ist,

$$\text{I.} \quad N \cdot 2\sqrt{P} = -\left\{1 - \left(\frac{2}{P}\right)\frac{1}{2}\right\} \log\{F(1)^2\}$$

$$\text{II.} \quad N \cdot 2\sqrt{P} = -\log\{cF(i)^2\}$$

$$\text{III.} \quad N \cdot 2\sqrt{2P} = \log\left\{\frac{F(j^3)^2}{F(j)^2}\right\}$$

$$\text{IV.} \quad N \cdot 2\sqrt{2P} = -\log\{c^2 F(j)^2 F(j^3)^2\}.$$

§. 106.

Nachdem der Werth der unendlichen Reihe N für alle Fälle bestimmt ist, in welchen die Determinante D durch kein Quadrat (ausser 1) theilbar ist, können wir nun die Anzahl h der Classen der ursprünglichen Formen der ersten Art in geschlossener Form angeben *).

A. Für *negative* Determinanten D ist (nach §. 97)

$$h = \frac{2\sqrt{-D}}{\pi} \cdot N,$$

mit Ausnahme des Falles $D = -1$, wo der Ausdruck rechter Hand zu verdoppeln ist. Hieraus ergeben sich folgende vier Resultate

$$\text{I.} \quad D = -P \equiv 1 \pmod{4};\quad h = \sum_0^4 \left(\frac{s}{P}\right)$$

$$\text{II.} \quad D = -P \equiv 3 \pmod{4};\quad h = 2\sum_0^2 \left(\frac{s}{P}\right)$$

$$\text{III.} \quad D = -2P \equiv 2 \pmod{8};\quad h = 2\sum_1^3 \left(\frac{s}{P}\right)$$

$$\text{IV.} \quad D = -2P \equiv 6 \pmod{8};\quad h = 2\left\{\sum_0^1 \left(\frac{s}{P}\right) - \sum_3^4 \left(\frac{s}{P}\right)\right\},$$

wo die Grenzen der Summationen sich immer auf den Werth $8s : P$

*) Vergl. *Kronecker: Ueber die Anzahl der verschiedenen Classen quadratischer Formen von negativer Determinante*, Crelle's Journal LVII. Daselbst findet man für negative Determinanten wesentlich neue Formeln, welche aus der Theorie der elliptischen Functionen abgeleitet sind.

beziehen*). Aus II. und IV. sind resp. die Fälle $D = -1$ und $D = -2$ auszunehmen, in welchen $h = 1$ ist.

B. Für *positive* Determinanten D ist (nach §. 99)

$$h \log(T + U\sqrt{D}) = N \,.\, 2\sqrt{D},$$

wo T, U die kleinsten positiven ganzen Zahlen bedeuten, welche der Gleichung

$$T^2 - DU^2 = 1$$

genügen und nach der angegebenen Methode (§. 84) stets gefunden werden können. Der Werth $N \,.\, 2\sqrt{D}$ ist am Schlusse des vorigen Paragraphen bestimmt; statt der dortigen Formeln kann man auch die folgenden aus der Gleichung (2) des vorigen Paragraphen ableiten:

I. $D = P \equiv 1 \pmod 4$

$$h \log(T + U\sqrt{P}) = -\left\{4 - 2\left(\frac{2}{P}\right)\right\} \sum_0^{\frac{1}{2}} \left(\frac{n}{P}\right) \log \sin \frac{n\pi}{P}$$

II. $D = P \equiv 3 \pmod 4$

$$h \log(T + U\sqrt{P}) = -\sum_0^{4} \left(\frac{-1}{n}\right)\left(\frac{n}{P}\right) \log \sin \frac{n\pi}{4P}$$

III. $D = 2P \equiv 2 \pmod 8$

$$h \log(T + U\sqrt{2P}) = -\sum_0^{8} \left(\frac{2}{n}\right)\left(\frac{n}{P}\right) \log \sin \frac{n\pi}{8P}$$

IV. $D = 2P \equiv 6 \pmod 8$

$$h \log(T + U\sqrt{2P}) = -\sum_0^{8} \left(\frac{-2}{n}\right)\left(\frac{n}{P}\right) \log \sin \frac{n\pi}{8P}$$

wo n alle relativen Primzahlen zu $2P$ durchlaufen muss, für welche $n:P$ zwischen den angegebenen Summationsgrenzen liegt. Die drei letzten Fälle lassen sich in der gemeinschaftlichen Formel

$$h \log(T + U\sqrt{D}) = -\sum \left(\frac{D}{n}\right) \log \sin \frac{n\pi}{4D}$$

zusammenfassen, wo n alle zwischen 0 und $4D$ liegenden relativen Primzahlen zu $4D$ durchlaufen muss.

*) Umgekehrt kann man diese Formeln benutzen, um die Vertheilung der Zahlen a und b auf die acht Octanten mit Hülfe der Classenanzahlen für die Determinanten $-P$ und $-2P$ zu bestimmen (Gauss' Werke Bd. II. 1863. p. 288).

§. 107.

Betrachten wir die so gewonnenen Resultate, so zeigt sich ein wesentlicher Unterschied zwischen den positiven und negativen Determinanten. Während nämlich der Ausdruck für die Classenanzahl bei einer negativen Determinante unmittelbar die Form einer *ganzen* Zahl hat — dass dieselbe zugleich *positiv* ist, hat freilich bis jetzt noch Niemand auf elementarem Wege nachgewiesen — so ist dies keineswegs unmittelbar ersichtlich bei den Ausdrücken, welche die Classenanzahl für eine positive Determinante darstellen. Es ist nun von hohem Interesse, dass mit Hülfe eines Satzes aus der von *Gauss* *) gegründeten Theorie der *Kreistheilung* (Supplement VII.) die obigen Ausdrücke für $h \log (T + U\sqrt{D})$ wirklich stets in die Form $\log (t + u\sqrt{D})$ übergeführt werden können, wo t, u ganze Zahlen bedeuten, welche der Gleichung $t^2 - Du^2 = 1$ genügen. Dies wollen wir jetzt nachweisen**).

Behalten wir die bisherigen Bezeichnungen bei, so können wir, wie im Supplement VII. gezeigt ist, stets

$$2A(x) = 2\prod (x - \theta^a) = Y(x) - i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P} \,.\, Z(x)$$

$$2B(x) = 2\prod (x - \theta^b) = Y(x) + i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P} \,.\, Z(x).$$

setzen, wo $\sqrt{P}$ positiv ist, und $Y(x)$, $Z(x)$ ganze Functionen von x bedeuten, deren Coefficienten ganze Zahlen sind. Zugleich ist

$$A(x)\,B(x) = \prod (x - \theta^s) = \frac{\prod (x^{\mu_1} - 1)}{\prod (x^{\mu_2} - 1)},$$

wo μ_1 jedes positive, μ_2 jedes negative Glied des entwickelten Productes

$$\varphi(P) = (p-1)(p'-1)(p''-1)\ldots = \Sigma\, \mu_1 - \Sigma\, \mu_2$$

bedeutet, und

$$F(x) = \prod (x - \theta^s)^{\left(\frac{s}{P}\right)} = \frac{A(x)}{B(x)}.$$

---

*) *D. A.* Sectio VII.

**) *Lejeune Dirichlet: Sur la manière de résoudre l'équation* $t^2 - pu^2 = 1$ *au moyen des fonctions circulaires* (Crelle's Journal XVII). Vergl. *Jacobi: Ueber die Kreistheilung und ihre Anwendung auf die Zahlentheorie* (Berliner Monatsberichte 1837).

Wir wenden uns nun, indem wir die am Schlusse des §. 105 gefundenen Ausdrücke für das Product $h \log(T + U\sqrt{D}) = N \cdot 2\sqrt{D}$ zu Grunde legen, zunächst dem Falle I. zu, in welchem $D = P \equiv 1 \pmod{4}$, und also

$$h \log(T + U\sqrt{P}) = -\left\{1 - \left(\frac{2}{P}\right)\frac{1}{2}\right\} \log\{F(1)^2\}$$

ist. Da nun

$$A(1)B(1) = \frac{\Pi \mu_1}{\Pi \mu_2} = P^\varkappa$$

ist, wo $\varkappa = 1$ oder $= 0$ ist, je nachdem P eine Primzahl oder zusammengesetzt ist (§. 138), so ergiebt sich

$$F(1) = \frac{A(1)}{B(1)} = \frac{P^\varkappa}{B(1)^2};$$

da ferner

$$2A(1) = y - z\sqrt{P}, \quad 2B(1) = y + z\sqrt{P}$$

ist, wo die ganzen Zahlen $Y(1)$, $Z(1)$ zur Abkürzung mit y, z bezeichnet sind, so wird

$$y^2 - Pz^2 = 4P^\varkappa,$$

und folglich muss, wenn P eine Primzahl ist, y durch P theilbar sein; mithin kann man in allen Fällen

$$y + z\sqrt{P} = (\alpha + \beta\sqrt{P})(\sqrt{P})^\varkappa$$

setzen, wo α, β ganze Zahlen bedeuten, welche der Gleichung

$$\alpha^2 - P\beta^2 = 4(-1)^\varkappa$$

genügen, und man erhält

$$(T + U\sqrt{P})^h = \left(\frac{\alpha + \beta\sqrt{P}}{2}\right)^{4-2\left(\frac{2}{P}\right)}.$$

Sind nun die Zahlen y, z gerade, was jedenfalls eintreten muss, wenn $P \equiv 1 \pmod{8}$ ist, so kann man $\alpha = 2\alpha'$, $\beta = 2\beta'$ setzen, wo die ganzen Zahlen α' β' der Gleichung

$$\alpha'^2 - P\beta'^2 = (-1)^\varkappa$$

genügen; setzt man ferner

$$(\alpha' + \beta'\sqrt{P})^{1+\varkappa} = t + u\sqrt{P},$$

so genügen die ganzen Zahlen t, u der Gleichung $t^2 - Pu^2 = 1$ und man erhält

$$(T + U\sqrt{P})^h = (t + u\sqrt{P})^{\left(2-\left(\frac{2}{P}\right)\right)(2-\varkappa)}.$$

Sind dagegen die Zahlen y, z und folglich auch α, β ungerade, was nur dann eintreten kann, wenn $P \equiv 5 \pmod{8}$ ist (z.B. wenn $P = 13$, während z.B. für $P = 37$ der frühere Fall Statt findet), so kann man

$$\left(\frac{\alpha + \beta \sqrt{P}}{2}\right)^3 = \alpha' + \beta' \sqrt{P}$$

setzen, wo α', β' ganze Zahlen sind, die der Gleichung

$$\alpha'^2 - P\beta'^2 = (-1)^x$$

genügen; setzt man nun wieder

$$(\alpha' + \beta' \sqrt{P})^{1+x} = t + u\sqrt{P},$$

so wird $t^2 - Pu^2 = 1$, und

$$(T + U\sqrt{P})^h = (t + u\sqrt{P})^{2-x}.$$

Es leuchtet ein, dass, wenn $P \equiv 5 \pmod{8}$ ist, der erste oder zweite Fall eintreten wird, je nachdem die Classenanzahl h durch 3 theilbar ist oder nicht (vergl. §. 99). Ebenso leicht erkennt man, dass in allen Fällen $h \equiv x \pmod{2}$, d. h. dass die Classenanzahl h ungerade oder gerade sein wird, je nachdem P eine Primzahl oder zusammengesetzt ist (vergl. §. 83. Anm.). Endlich mag noch bemerkt werden, dass die Zahlen y, z beide positiv sind; da nämlich $P \equiv 1 \pmod{4}$, so zerfallen die Zahlen a in Paare von der Form a und $-a$, ebenso die Zahlen b in Paare von der Form b und $-b$, und folglich sind $A(1)$, $B(1)$ und $A(1) + B(1) = y$ positiv; da ferner

$$\left\{2 - \left(\frac{2}{P}\right)\right\} \{\log B(1) - \log A(1)\} = h \log(T + U\sqrt{P})$$

positiv ist, weil h positiv, $T + U\sqrt{P} > 1$ ist, so muss $B(1) > A(1)$, und folglich z positiv sein: ein Resultat, das bisher auf anderm Wege noch nicht bewiesen ist.

§. 108.

Für den zweiten Fall $D = P \equiv 3 \pmod{4}$ haben wir oben das Resultat

$$h \log(T + U\sqrt{P}) = -\log\{cF(i)^2\}$$

erhalten; da nun, wenn m irgend eine ungerade Zahl bedeutet,

$$\frac{i^m - 1}{i - 1} = i^{1/4(m-1)^2}$$

ist, und da ferner

$$\Sigma \mu_1 - \Sigma \mu_2 = (p-1)(p'-1)(p''-1)\dots$$
$$\Sigma \mu_1^2 - \Sigma \mu_2^2 = (p^2-1)(p'^2-1)(p''^2-1)\dots$$

ist, so findet man leicht

$$A(i)\,B(i) = \frac{\Pi(i^{\mu_1}-1)}{\Pi(i^{\mu_2}-1)} = i^{\varkappa},$$

wo $\varkappa$ wieder $= 1$ oder $= 0$ ist, je nachdem P eine Primzahl oder zusammengesetzt ist. Folglich wird

$$F(i) = \frac{A(i)}{B(i)} = \frac{i^{\varkappa}}{B(i)^2},$$

und also, da $c^3 = 1$ ist,

$$(T + U\sqrt{P})^h = c^2\,(-1)^{\varkappa} B(i)^4.$$

Mit Ausnahme des Falles $P = 3$ ist nun (nach §. 140) $c = 1$, und

$$(-x)^{\tau} B\left(\frac{1}{x}\right) = A(x), \quad (-x)^{\tau} A\left(\frac{1}{x}\right) = B(x),$$

wo $\varphi(P) = 2\tau$ gesetzt ist, folglich

$$i^{\tau} B(i) = A(-i), \quad i^{\tau} A(i) = B(-i),$$

also auch

$$i^{\tau}.\,Y(i) = Y(-i), \quad i^{\tau}.\,iZ(i) = -\,iZ(-i);$$

berücksichtigt man nun, dass

$$i^{\tau} = -\left(\frac{2}{P}\right) i \quad \text{oder} \quad = 1$$

ist, je nachdem P eine Primzahl oder zusammengesetzt ist, so folgt hieraus, dass man

$$Y(i) = \left(1 + \left(\frac{2}{P}\right) i\right)^{\varkappa} y, \quad iZ(i) = \left(1 + \left(\frac{2}{P}\right) i\right)^{\varkappa} z,$$

also

$$2A(i) = \left(1 + \left(\frac{2}{P}\right) i\right)^{\varkappa} (y - z\sqrt{P}), \quad 2B(i) = \left(1 + \left(\frac{2}{P}\right) i\right)^{\varkappa} (y + z\sqrt{P})$$

setzen kann, wo y, z ganze Zahlen bedeuten, welche der durch Multiplication entstehenden Gleichung

$$y^2 - Pz^2 = \left(\frac{2}{P^{\varkappa}}\right) 2^{2-\varkappa}$$

genügen; hieraus folgt weiter, dass man

$$(y + z\sqrt{P})^{1+\varkappa} = 2(t + u\sqrt{P})$$

setzen kann, wo t, u ganze Zahlen bedeuten, welche der Gleichung $t^2 - Pu^2 = 1$ genügen. Zugleich wird

$$B(i)^{1+\varkappa} = \left(\frac{2}{P^\varkappa}\right) i^\varkappa (t + u\sqrt{P}),$$

und folglich

$$(T + U\sqrt{P})^h = (t + u\sqrt{P})^{4-2\varkappa}.$$

Wir erwähnen, dass $h \equiv 2\varkappa$ (mod. 4) ist, und dass die Zahlen y, z stets dasselbe Vorzeichen haben.

In dem bisher ausgeschlossenen Fall $P = 3$ ist $T = 2$, $U = 1$, $c = \theta$, $B(i) = i - \theta^2$, woraus leicht folgt, dass

$$\frac{1}{cF(i)^2} = c^2(-1)^\varkappa B(i)^4 = (2 + \sqrt{3})^2,$$

also $h = 2$ ist.

§. 109.

Für den dritten Fall $D = 2P \equiv 2$ (mod. 8) haben wir oben

$$h \log(T + U\sqrt{2P}) = \log\left\{\frac{F(j^3)^2}{F(j)^2}\right\}$$

gefunden. Berücksichtigt man nun, dass, wenn m irgend eine ungerade Zahl bedeutet,

$$\frac{(j^m - 1)\,(j^{3m} - 1)}{(j - 1)\,(j^3 - 1)} = \left(\frac{-2}{m}\right)$$

ist, so findet man

$$A(j)B(j)A(j^3)B(j^3) = \frac{\Pi\,(j^{\mu_1} - 1)\,(j^{3\mu_1} - 1)}{\Pi\,(j^{\mu_2} - 1)\,(j^{3\mu_2} - 1)} = \left(\frac{-2}{P^\varkappa}\right),$$

und folglich

$$(T + U\sqrt{2P})^h = A(j^3)^4 B(j)^4,$$

wo $\varkappa$ wieder $= 1$ oder $= 0$, je nachdem P eine Primzahl oder zusammengesetzt ist. Da nun $P \equiv 1$ (mod. 4), und also $Y(j) = j^\tau Y(j^{-1})$, $Z(j) = j^\tau Z(j^{-1})$ ist (§. 140), so kann man

$$Y(j) = j^{1/2\tau}\{y' + y''(j - j^3)\}, \quad Z(j) = j^{1/2\tau}\{z' + z''(j - j^3)\}$$

setzen, wo y', y'', z', z'' ganze Zahlen bedeuten; da ferner $j - j^3 = \sqrt{2}$ ist, so erhält man, wenn man

$$\alpha = (-1)^{1/2\tau}\{y'^2 - 2y''^2 - P(z'^2 - 2z''^2)\},$$
$$\beta = (-1)^{1/2\tau}.2(y'z'' - y''z')$$

setzt,

$$4A(j^3)B(j) = \alpha + \beta\sqrt{2P}, \quad 4A(j)B(j^3) = \alpha - \beta\sqrt{2P},$$

wo die ganzen Zahlen α, β der Gleichung

$$\alpha^2 - 2P\beta^2 = 16\left(\frac{-2}{P^\varkappa}\right)$$

genügen und folglich beide durch 4 theilbar sind. Man kann daher

$$A(j^3)B(j) = y + z\sqrt{2P}$$

setzen, wo die ganzen Zahlen y, z der Gleichung

$$y^2 - 2Pz^2 = \left(\frac{-2}{P^\varkappa}\right)$$

genügen, und es ist

$$(T + U\sqrt{2P})^h = (y + z\sqrt{2P})^4.$$

Hieraus folgt, dass $h \equiv 2 \pmod{4}$, falls P eine Primzahl von der Form $8n + 5$, sonst aber $h \equiv 0 \pmod{4}$ ist.

In dem bisher ausgeschlossenen Falle $D = 2$ war $N\sqrt{D} = \log(1 + \sqrt{2})$; da ferner $T = 3$, $U = 2$ ist, so folgt

$$h \log(3 + 2\sqrt{2}) = 2\log(1 + \sqrt{2}),$$

also $h = 1$.

§. 110.

Für den vierten Fall $D = 2P \equiv 6 \pmod{8}$ haben wir oben (§§. 105, 106) das Resultat

$$h \log(T + U\sqrt{2P}) = -\log\{c^2 F(j)^2 F(j^3)\}^2$$

gefunden, welches vermöge der Gleichung

$$A(j)B(j)A(j^3)B(j^3) = \left(\frac{-2}{P^\varkappa}\right)$$

in

$$(T + U\sqrt{2P})^h = c\,B(j)^4 B(j^3)^4$$

übergeht, weil $c^3 = 1$ ist. Lassen wir den Fall $P = 3$ unberücksichtigt, so ist (nach §. 140) $c = 1$, und $Y(j) = (-j)^\tau\, Y(j^{-1})$, $-Z(j) = (-j)^\tau\, Z(j^{-1})$; da ferner τ ungerade oder durch 4 theilbar ist, je nachdem $\varkappa = 1$ oder $= 0$, d. h. je nachdem P eine Primzahl oder zusammengesetzt ist, so kann man

$$Y(j) = (j^{\frac{1}{2}\tau(1+\varkappa)} - \varkappa)\,(y' + y''(j - j^3))$$
$$j^2 Z(j) = (j^{\frac{1}{2}\tau(1+\varkappa)} - \varkappa)\,(z' + z''(j - j^3))$$

setzen, wo y', y'', z', z'' ganze Zahlen bedeuten; berücksichtigt man, dass $j - j^3 = \sqrt{2}$ ist, und setzt

$$\alpha = y'^2 - Pz'^2 - 2y''^2 + 2Pz''^2$$
$$\beta = 2(y'z'' - z'y''),$$

so erhält man

$$4A(j)A(j^3) = (-j^\tau - j^{3\tau})^\varkappa (\alpha - \beta\sqrt{2P})$$
$$4B(j)B(j^3) = (-j^\tau - j^{3\tau})^\varkappa (\alpha + \beta\sqrt{2P}),$$

wo die ganzen Zahlen α, β der durch Multiplication entstehenden Gleichung

$$\alpha^2 - 2P\beta^2 = \left(\frac{-2}{P^\varkappa}\right)(-2)^{4-\varkappa}$$

genügen; man kann daher

$$(\alpha + \beta\sqrt{2P})^{1+\varkappa} = 2^{2+\varkappa}(t + u\sqrt{2P})$$

setzen, wo die ganzen Zahlen t, u der Gleichung $t^2 - 2Pu^2 = 1$ genügen; dann wird

$$B(j)^{1+\varkappa} B(j^3)^{1+\varkappa} = (-1)^\varkappa (t + u\sqrt{2P})$$

und folglich

$$(T + U\sqrt{2P})^h = (t + u\sqrt{2P})^{4-2\varkappa},$$

woraus leicht folgt, dass $h \equiv 2\varkappa \pmod{4}$ ist.

In dem ausgeschlossenen Fall $P = 3$ ist $c = \theta = \theta^4$, $T = 5$, $U = 2$, und man erhält

$$\theta B(j)B(j^3) = \theta(j - \theta^2)(j^3 - \theta^2) = -i(\sqrt{2} + \sqrt{3})$$
$$\theta^2 B(j)^2 B(j^3)^2 = -(5 + 2\sqrt{6}) = -(T + U\sqrt{2P})$$

und hieraus $h = 2$.

SUPPLEMENTE.

I. Ueber einige Sätze aus der Theorie der Kreistheilung von Gauss.

§. 111.

Wir schicken zunächst ein Lemma aus der Theorie der Fourier'schen Reihen voraus, deren Glieder nach den Cosinus der successiven Vielfachen eines Winkels fortschreiten; es wird in derselben nachgewiesen*), dass für alle reellen Werthe von x zwischen $x = 0$ und $x = \pi$ mit Einschluss dieser Grenzen stets

$$\varphi(x) = \tfrac{1}{2} a_0 + a_1 \cos x + a_2 \cos 2x + a_3 \cos 3x + \cdots$$

ist, wenn $\varphi(x)$ eine innerhalb dieses Intervalles endliche und stetige Function bedeutet, welche nicht unendlich viele Maxima und Minima hat, und wo die Coefficienten $a_0, a_1, a_2 \ldots$ durch die Gleichung

$$a_s = \frac{2}{\pi} \int_0^\pi \varphi(x) \cos sx \, dx$$

bestimmt werden. Hieraus folgt für $x = 0$

$$\pi \varphi(0) = \sum_{-\infty}^{+\infty} \int_0^\pi \varphi(x) \cos sx \, dx,$$

wo das Summenzeichen sich auf den Buchstaben s bezieht, für welchen Null und alle ganzen positiven und negativen Zahlwerthe der Reihe nach einzusetzen sind. Auf diesen der genannten Theorie entlehnten Satz stützen wir uns im Folgenden.

*) *Dirichlet: Sur la convergence des séries etc.* (Crelle's Journal IV); derselbe Beweis ist vereinfacht im Repertorium der Physik von Dove und Moser. Bd. I. Vergl. *B. Riemann: Ueber die Darstellbarkeit einer Function durch eine trigonometrische Reihe.* 1867.

Zunächst verallgemeinern wir denselben, indem wir das Integral

$$\int_0^{2h\pi} f(x)\cos sx\,dx$$

betrachten, in welchem h eine positive ganze Zahl, s eine positive oder negative ganze Zahl, und $f(x)$ eine Function bedeutet, welche innerhalb des Integrationsgebietes den obigen Bedingungen genügt. Man kann dasselbe in $2h$ Integrale von der Form

$$\int_{r\pi}^{(r+1)\pi} f(x)\cos sx\,dx$$

zerlegen, wo für r der Reihe nach die Zahlen $0, 1, 2 \ldots$ bis $2h-1$ zu setzen sind; je nachdem r eine gerade oder ungerade Zahl ist, ersetzen wir die Integrationsvariabele x durch $r\pi+x$, oder durch $(r+1)\pi-x$; dadurch geht das vorstehende Integral in

$$\int_0^{\pi} f(r\pi+x)\cos sx\,dx, \text{ oder in} \int_0^{\pi} f((r+1)\pi-x)\cos sx\,dx$$

über, und hieraus ergiebt sich zufolge des obigen Satzes entsprechend

$$\sum_{-\infty}^{+\infty}\int_{r\pi}^{(r+1)\pi} f(x)\cos sx\,dx = \pi f(r\pi), \quad \text{oder} = \pi f((r+1)\pi),$$

wo die Summe links sich wieder auf alle ganzen Zahlen s bezieht. Setzt man hierin für r die ganzen Zahlen $0, 1, 2 \ldots 2h-1$, und addirt die so entstehenden Gleichungen, so erhält man den Satz

$$2\pi\{\tfrac{1}{2}f(0)+f(2\pi)+f(4\pi)+\cdots+f(2(h-1)\pi)+\tfrac{1}{2}f(2h\pi)\}$$
$$=\sum_{-\infty}^{+\infty}\int_0^{2h\pi} f(x)\cos sx\,dx.$$

§. 112.

Wir beschäftigen uns nun mit den beiden folgenden bestimmten Integralen

$$p = \int_{-\infty}^{+\infty} \cos(x^2)\, dx, \quad q = \int_{-\infty}^{+\infty} \sin(x^2)\, dx;$$

dass dieselben wirklich bestimmte endliche Werthe besitzen, obgleich die Functionen unter den Integralzeichen für unendlich grosse Werthe von x nicht unendlich klein werden, erkennt man leicht durch die Transformationen

$$p = 2\int_0^{\infty} \cos(x^2)\, dx = \int_0^{\infty} \frac{\cos y}{\sqrt{y}}\, dy$$

$$q = 2\int_0^{\infty} \sin(x^2)\, dx = \int_0^{\infty} \frac{\sin y}{\sqrt{y}}\, dy;$$

denn zerlegt man das ganze unendliche Integrationsgebiet der positiven Variabeln y in solche Intervalle, in deren jedem die unter dem Integralzeichen befindliche Function ihr Zeichen nicht ändert, so ergiebt sich, dass die Bestandtheile, welche diesen Intervallen entsprechen, eine unendliche Reihe bilden, deren Glieder abwechselnde Zeichen haben und dem absoluten Werthe nach beständig und zwar ins Unendliche abnehmen; woraus folgt, dass diese Reihe, sowohl bei dem Integrale p, wie bei q, eine convergente ist. Für unsern Zweck genügt dieser Nachweis der Endlichkeit von p und q; die numerischen Werthe dieser Integrale werden sich von selbst aus der folgenden Untersuchung ergeben*).

Beide Integrale bilden nur specielle Fälle des folgenden

---

*) *Dirichlet: Recherches sur diverses appl.* etc. §. 9. Vergl. *Dirichlet: Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies* (Crelle's Journal XVII).

$$\varDelta = \int_{-\infty}^{+\infty} \cos(\delta + x^2)\, dx = p \cos \delta - q \sin \delta,$$

wo δ eine beliebige Constante bedeutet; bezeichnen wir ferner mit α eine beliebige positive Constante und mit $\sqrt{\alpha}$ die *positiv* genommene Quadratwurzel aus α, so ergiebt sich, wenn man die Integrationsvariabele x durch $x\sqrt{\alpha}$ ersetzt, folgende Gleichung

$$\frac{\varDelta}{\sqrt{\alpha}} = \int_{-\infty}^{+\infty} \cos(\delta + \alpha x^2)\, dx$$

(wäre $\sqrt{\alpha}$ negativ, so müsste man auch in dem Integrale rechter Hand die beiden Grenzen mit einander vertauschen). Wir führen nun eine zweite positive Constante β ein, und zerlegen das vorstehende Integral in unendlich viele Bestandtheile von der Form

$$\int_{s\beta}^{(s+1)\beta} \cos(\delta + \alpha x^2)\, dx,$$

wo für s successive alle ganzen Zahlen von $-\infty$ bis $+\infty$ einzusetzen sind; in jedem einzelnen solchen Integrale ersetzen wir die Integrationsvariabele x durch $s\beta + x$, wodurch es in das folgende übergeht

$$\int_{0}^{\beta} \cos(\delta + \alpha s^2 \beta^2 + 2\alpha s \beta x + \alpha x^2)\, dx.$$

Wir verfügen nun über die beiden bis jetzt ganz willkürlichen positiven Constanten α und β folgendermaassen: unter m verstehen wir irgend eine positive ganze Zahl, und setzen $\alpha\beta^2 = 2m\pi$, $2\alpha\beta = 1$, d. h. also

$$\beta = 4m\pi, \quad \alpha = \frac{1}{8m\pi}.$$

Da nun s eine ganze Zahl ist, so wird

$$\cos(\delta + \alpha s^2\beta^2 + 2\alpha s\beta x + \alpha x^2) = \cos(\delta + sx + \alpha x^2)$$

$$= \cos\left(\delta + \frac{x^2}{8m\pi}\right) \cos sx - \sin\left(\delta + \frac{x^2}{8m\pi}\right) \sin sx,$$

und folglich

$$\int_{s\beta}^{(s+1)\beta} \cos(\delta + \alpha x^2)\, dx$$

$$= \int_0^{4m\pi} \cos\left(\delta + \frac{x^2}{8m\pi}\right) \cos sx\, dx - \int_0^{4m\pi} \sin\left(\delta + \frac{x^2}{8m\pi}\right) \sin sx\, dx.$$

Das zweite Integral rechter Hand, welches unter dem Integralzeichen den Factor $\sin sx$ enthält, verschwindet offenbar für $s = 0$, und nimmt für je zwei gleiche, aber entgegengesetzte Werthe von s ebenfalls gleiche, aber entgegengesetzte Werthe an. Summiren wir daher den vorstehenden Ausdruck für alle ganzen Zahlwerthe s von $-\infty$ bis $+\infty$, so ergiebt sich

$$\frac{\varDelta}{\sqrt{\alpha}} = \varDelta\sqrt{8m\pi} = \sum_{-\infty}^{+\infty} \int_0^{4m\pi} \cos\left(\delta + \frac{x^2}{8m\pi}\right) \cos sx\, dx.$$

Die rechte Seite dieser Gleichung ist nun genau so gebaut wie in dem Satze am Schlusse des vorhergehenden Paragraphen; setzen wir zur Abkürzung

$$f(x) = \cos\left(\delta + \frac{x^2}{8m\pi}\right),$$

so erhalten wir

$$\varDelta\sqrt{8m\pi} = 2\pi\{\tfrac{1}{2}f(0) + f(2\pi) + \cdots + f(2(2m-1)\pi) + \tfrac{1}{2}f(4m\pi)\},$$

wo links die Quadratwurzel

$$\sqrt{8m\pi} = \frac{1}{\sqrt{\alpha}}$$

positiv zu nehmen ist. Nun ist ferner, wenn s irgend eine ganze Zahl bedeutet,

$$f(4m\pi + 2s\pi) = f(2s\pi),$$

also

$$f(2s\pi) = \tfrac{1}{2}f(2s\pi) + \tfrac{1}{2}f(4m\pi + 2s\pi);$$

mithin kann die in den Parenthesen eingeschlossene Summe auch in die Form

$$\tfrac{1}{2}\sum f(2s\pi)$$

gebracht werden, wo der Buchstabe s die Zahlen

$$0, 1, 2 \ldots (4m-1)$$

oder irgend ein anderes vollständiges Restsystem in Bezug auf den Modul $4m$ durchlaufen muss; und man erhält also

$$\Delta\sqrt{8m\pi} = \pi \sum \cos\left(\delta + s^2 \frac{\pi}{2m}\right).$$

Setzt man ferner $4m = n$, so dass n irgend eine ganze positive, aber durch 4 theilbare Zahl bedeutet, und bezeichnet man mit $\sqrt{n}$ und $\sqrt{\frac{1}{2}\pi}$ die *positiv* genommenen Quadratwurzeln aus n und $\frac{1}{2}\pi$, so nimmt die Gleichung folgende Gestalt an

$$\Delta\sqrt{n} = \sqrt{\tfrac{1}{2}\pi}\cdot\sum\cos\left(\delta + s^2\cdot\frac{2\pi}{n}\right),$$

wo s ein vollständiges Restsystem in Bezug auf den Modul n durchlaufen muss. Nun ist

$$\Delta = p\cos\delta - q\sin\delta,$$

wo p, q die obigen Integralwerthe bedeuten, die von n und dem willkürlichen δ ganz unabhängig sind; wir können daher p und q durch eine specielle Annahme für n, am einfachsten durch die Annahme $n = 4$ bestimmen; auf diese Weise erhalten wir

$$2(p\cos\delta - q\sin\delta) = 2(\cos\delta - \sin\delta)\sqrt{\tfrac{1}{2}\pi},$$

und in Folge der Willkürlichkeit von δ

$$p = q = \sqrt{\tfrac{1}{2}\pi}.$$

Nachdem so die Werthe von p und q gefunden sind, nimmt unsere obige Gleichung folgende Gestalt an

$$\sum\cos\left(\delta + s^2\frac{2\pi}{n}\right) = (\cos\delta - \sin\delta)\sqrt{n},$$

und sie zerfällt in die beiden folgenden:

$$\sum\cos\left(s^2\frac{2\pi}{n}\right) = \sqrt{n}$$

$$\sum\sin\left(s^2\frac{2\pi}{n}\right) = \sqrt{n};$$

hierin bedeutet also n jede beliebige ganze positive Zahl, welche $\equiv 0 \pmod{4}$ ist, und $\sqrt{n}$ die *positiv* genommene Quadratwurzel aus n. Bezeichnet man zur Abkürzung $\sqrt{-1}$ mit i, und, wie gewöhnlich, mit e die Basis des natürlichen Logarithmensystems, so kann man beide Gleichungen in die eine Gleichung

$$\sum e^{s^2\cdot\frac{2\pi i}{n}} = (1+i)\sqrt{n}$$

zusammenziehen, in welcher der Buchstabe s ein vollständiges Restsystem (mod. n) zu durchlaufen hat.

§. 113.

Wir wollen jetzt Summen betrachten, welche die vorstehende als speciellen Fall enthalten; wir bezeichnen mit n irgend eine ganze positive Zahl, mit h irgend eine positive oder negative ganze Zahl, und setzen zur Abkürzung

$$\Sigma\, e^{s^2 \frac{2h\pi i}{n}} = \varphi(h, n),$$

wo der Summationsbuchstabe s irgend ein vollständiges Restsystem in Bezug auf den Modulus n durchlaufen muss. Mit Hülfe dieser Bezeichnungsweise können wir den im vorigen Paragraphen bewiesenen Satz in folgender Weise ausdrücken:

$$\varphi(1, n) = (1 + i)\sqrt{n}, \quad \text{wenn} \quad n \equiv 0 \pmod{4}.$$

Der Ausdruck $\varphi(h,n)$ besitzt nun die folgenden drei Eigenschaften:

1. Ist $h \equiv h' \pmod{n}$, so ist

$$\varphi(h, n) = \varphi(h', n);$$

dies folgt unmittelbar daraus, dass für jeden ganzzahligen Werth von s stets

$$e^{s^2 \frac{2h\pi i}{n}} = e^{s^2 \frac{2h'\pi i}{n}}$$

ist.

2. Ist a relative Primzahl gegen n, so ist

$$\varphi(h a^2, n) = \varphi(h, n);$$

denn es ist

$$\varphi(h a^2, n) = \Sigma\, e^{(as)^2 \frac{2h\pi i}{n}},$$

und wenn s ein vollständiges Restsystem nach dem Modul n durchläuft, so gilt (nach §. 18) dasselbe von as.

3. Sind m, n irgend zwei relative Primzahlen, und beide positiv, so ist

$$\varphi(hm, n)\, \varphi(hn, m) = \varphi(h, mn).$$

Es ist nämlich

$$\varphi(hm, n) = \Sigma\, e^{s^2 \frac{2hm\pi i}{n}},\quad \varphi(hn, m) = \Sigma\, e^{t^2 \frac{2hn\pi i}{m}},$$

wo die Buchstaben s, t vollständige Restsysteme resp. in Bezug auf die Moduln n, m durchlaufen müssen; und folglich ist

$$\varphi(hm, n)\, \varphi(hn, m) = \Sigma\, e^{\left(\frac{ms^2}{n} + \frac{nt^2}{m}\right) 2h\pi i},$$

wo das Summenzeichen rechter Hand sich auf alle mn Combinationen jedes Werthes von s mit jedem Werthe von t bezieht. Da nun

$$\frac{ms^2}{n} + \frac{nt^2}{m} = \frac{(ms + nt)^2}{mn} - 2st$$

ist, und alle Multipla von $2\pi i$ im Exponenten fortgelassen werden können, so ist auch

$$\varphi(hm, n)\, \varphi(hn, m) = \Sigma\, e^{(ms+nt)^2 \frac{2h\pi i}{mn}},$$

wo das Summenzeichen sich wieder auf sämmtliche Werthe von s und t bezieht. Setzt man nun

$$ms + nt = r,$$

so nimmt r, wenn s und t alle ihnen zukommenden Werthe durchlaufen, im Ganzen mn Werthe an, und zwar sind diese alle incongruent nach dem Modulus mn; denn aus

$$ms + nt \equiv ms' + nt' \pmod{mn}$$

folgt

$$ms \equiv ms' \pmod{n},\quad nt \equiv nt' \pmod{m}$$

und folglich, da m und n relative Primzahlen sind,

$$s \equiv s' \pmod{n},\quad t \equiv t' \pmod{m};$$

d. h. die Zahl r nimmt nur dann Werthe an, welche nach dem Modul mn congruent sind, wenn die Werthe von s congruent nach dem Modul n, und gleichzeitig die Werthe von t congruent nach dem Modul m sind. Den mn verschiedenen Combinationen von s und t correspondiren daher mn Werthe von r, welche nach dem Modul mn incongruent sind, und folglich bilden diese Werthe von r ein vollständiges Restsystem nach dem Modul mn. Es ist folglich

$$\varphi(hm, n)\, \varphi(hn, m) = \Sigma\, e^{r^2 \frac{2h\pi i}{mn}} = \varphi(h, mn),$$

was zu beweisen war.

§. 114.

Mit Hülfe dieser Sätze können wir nun den Werth von $\varphi(1,n)$, welcher für den Fall, dass $n \equiv 0 \pmod{4}$ ist, schon in §. 112 gefunden ist, auch für alle andern Werthe der Zahl n bestimmen. Ist zunächst n irgend eine *ungerade* Zahl, so nehmen wir in dem letzten Satz des vorigen Paragraphen

$$h = 1, \quad m = 4,$$

und erhalten

$$\varphi(4, n)\, \varphi(n, 4) = \varphi(1, 4n);$$

nun ist nach dem zweiten Satze des vorigen Paragraphen

$$\varphi(4, n) = \varphi(2^2, n) = \varphi(1, n);$$

ferner ist

$$\varphi(n, 4) = 2(1 + i^n),$$

und nach dem in §. 112 gefundenen Resultat

$$\varphi(1, 4n) = (1+i)\sqrt{4n} = 2(1+i)\sqrt{n},$$

wo die Quadratwurzel $\sqrt{n}$ wieder positiv genommen werden muss. Hieraus ergiebt sich also

$$\varphi(1, n) \,.\, 2(1 + i^n) = 2(1+i)\sqrt{n}$$

oder

$$\varphi(1, n) = \frac{1+i}{1+i^n}\sqrt{n};$$

je nachdem nun $n \equiv 1$ oder $\equiv 3 \pmod{4}$ ist, wird

$$i^n = i \quad \text{oder} \quad = -i$$

und folglich

$$\frac{1+i}{1+i^n} = 1 \quad \text{oder} \quad = \frac{1+i}{1-i} = i,$$

also

$$\varphi(1, n) = \sqrt{n} \quad \text{oder} \quad = i\sqrt{n};$$

diese beiden Fälle lassen sich aber in die eine Formel

$$\varphi(1, n) = i^{\frac{1}{4}(n-1)^2}\sqrt{n}$$

zusammenfassen.

Ist endlich n durch 2, aber nicht durch 4 theilbar, also das Doppelte einer ungeraden Zahl, so setzen wir in dem dritten Satze des vorigen Paragraphen $h = 1$, ferner $m = 2$, und $\frac{1}{2}n$ statt n, wodurch allen Bedingungen desselben Genüge geschieht, und erhalten

$$\varphi(2, \tfrac{1}{2}n)\, \varphi(\tfrac{1}{2}n, 2) = \varphi(1, n);$$

nun ist aber

$$\varphi(\tfrac{1}{2}n, 2) = 0,$$

und folglich auch

$$\varphi(1, n) = 0.$$

Wir wollen die so gewonnenen Resultate in folgender Tabelle zusammenfassen:

$$\begin{aligned} \varphi(1, n) &= (1 + i)\sqrt{n}, && \text{wenn} \quad n \equiv 0 \pmod{4} \\ \varphi(1, n) &= i^{\frac{1}{4}(n-1)^2}\sqrt{n}, && \text{wenn} \quad n \equiv 1 \pmod{2} \\ \varphi(1, n) &= 0, && \text{wenn} \quad n \equiv 2 \pmod{4}. \end{aligned}$$

Von der grössten Wichtigkeit ist aber die Bemerkung, dass die in den beiden ersten Formeln vorkommende Quadratwurzel $\sqrt{n}$ durchaus *positiv* genommen werden muss, wie es sich bei der Untersuchung in §. 112 herausgestellt hat. Ohne diese nähere Bestimmung würden die vorstehenden Sätze sich auf viel einfachere Art beweisen lassen; *Gauss* wurde zuerst in seiner Theorie der Kreistheilung auf die Betrachtung solcher Summen geführt*); es ergiebt sich dort ohne Schwierigkeit der Werth des Quadrates derselben; der viel tiefer liegenden Bestimmung des Vorzeichens der Quadratwurzel widmete er aber eine besondere Abhandlung**), in welcher er auf einem, von dem hier (in §. 112) eingeschlagenen gänzlich verschiedenen Wege, nämlich durch rein algebraische Zerlegung dieser Summen in Producte, vollständig zum Ziele gelangte.

---

*) *D. A.* art. 356.

**) *Summatio quarumdam serierum singularium.* 1808.

§. 115.

Wir suchen nun den Werth von $\varphi(h, n)$ auch für beliebige Werthe von h zu bestimmen, beschränken uns dabei aber auf den Fall, dass n eine ungerade Primzahl ist, die wir mit p bezeichnen wollen. Bezeichnen wir mit α die sämmtlichen $\frac{1}{2}(p-1)$ incongruenten quadratischen Reste von p, mit β die $\frac{1}{2}(p-1)$ quadratischen Nichtreste, so ist (nach §. 33)

$$\varphi(h, p) = \Sigma\, e^{s^2 \frac{2h\pi i}{p}} = 1 + 2\, \Sigma\, e^{\alpha \frac{2h\pi i}{p}};$$

da ferner

$$1 + \Sigma\, e^{\alpha \frac{2h\pi i}{p}} + \Sigma\, e^{\beta \frac{2h\pi i}{p}} = \Sigma\, e^{s \frac{2h\pi i}{p}} = 0$$

ist, sobald h nicht durch p theilbar ist, so können wir für diesen Fall mit Benutzung des Legendre'schen Symbols

$$\varphi(h, p) = \Sigma\, e^{\alpha \frac{2h\pi i}{p}} - \Sigma\, e^{\beta \frac{2h\pi i}{p}} = \Sigma \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}}$$

setzen, wo s die Werthe $1, 2 \ldots (p-1)$ durchläuft. Da ferner

$$\left(\frac{hs}{p}\right) = \left(\frac{h}{p}\right)\left(\frac{s}{p}\right),\quad \left(\frac{h}{p}\right)\left(\frac{h}{p}\right) = 1$$

ist, so wird

$$\varphi(h,p) = \left(\frac{h}{p}\right) \Sigma \left(\frac{hs}{p}\right) e^{hs \cdot \frac{2\pi i}{p}},$$

oder, da h nicht theilbar durch p ist, und folglich hs gleichzeitig mit s ein vollständiges Restsystem nach dem Modul p durchläuft (mit Ausschluss der Zahl $\equiv 0$),

$$\varphi(h, p) = \left(\frac{h}{p}\right) \Sigma \left(\frac{s}{p}\right) e^{s \frac{2\pi i}{p}};$$

für $h = 1$ ergiebt sich

$$\varphi(1, p) = \Sigma \left(\frac{s}{p}\right) e^{s \frac{2\pi i}{p}}$$

und folglich (nach §. 114)

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p},$$

wo die Quadratwurzel $\sqrt{p}$ wieder positiv zu nehmen ist. (Wenn h durch p theilbar ist, so ergiebt sich unmittelbar aus der Definition dieser Summen $\varphi(h, p) = p$.)

Aus dem vorstehenden Resultate in Verbindung mit dem dritten Satze des §. 113 lässt sich nun auf ganz einfache Weise das Reciprocitätsgesetz in der Theorie der quadratischen Reste (§. 42) für je zwei positive ungerade Primzahlen p und q ableiten. Es ist nämlich

$$\varphi(q, p) = \left(\frac{q}{p}\right) i^{1/4(p-1)^2} \sqrt{p},$$

und ebenso

$$\varphi(p, q) = \left(\frac{p}{q}\right) i^{1/4(q-1)^2} \sqrt{q},$$

und nach dem vorhergehenden Paragraphen

$$\varphi(1, pq) = i^{1/4(pq-1)^2} \sqrt{pq},$$

und zwar sind alle Quadratwurzeln *positiv* zu nehmen, woraus folgt, dass

$$\sqrt{pq} = \sqrt{p}\sqrt{q}$$

ist. Nach dem dritten Satze des §. 113 ist nun

$$\varphi(p, q)\, \varphi(q, p) = \varphi(1, pq),$$

folglich

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) i^{1/4(p-1)^2 + 1/4(q-1)^2} \sqrt{p}\, \sqrt{q} = i^{1/4(pq-1)^2} \sqrt{pq},$$

und also

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{\lambda},$$

wo zur Abkürzung λ für

$$\frac{(pq-1)^2 - (p-1)^2 - (q-1)^2}{4} = \frac{p-1}{2}\,\frac{q-1}{2}\left\{(p+1)(q+1) - 2\right\}$$

gesetzt ist; da nun

$$(p+1)(q+1) - 2 \equiv 2 \pmod{4}$$

ist, so erhalten wir

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = i^{1/2(p-1)(q-1)} = (-1)^{1/2(p-1) \cdot 1/2(q-1)},$$

womit der Reciprocitätssatz von Neuem bewiesen ist. Dieser Beweis rührt ebenfalls von *Gauss* her*).

*) *Summatio quarumdam serierum singularium.* 1808.

Auf ganz ähnliche Art lassen sich die Sätze (§§. 40, 41) über die Zahlen -1 und 2 beweisen. Aus dem obigen Satze

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) i^{1/4(p-1)^2} \sqrt{p}$$

folgt nämlich

$$\varphi(-1, p) = \left(\frac{-1}{p}\right) i^{1/4(p-1)^2} \sqrt{p};$$

andererseits ist

$$\varphi(-1, p) = \Sigma\, e^{s^2 \frac{2\pi(-i)}{p}},$$

und hieraus folgt, dass $\varphi(-1, p)$ durch Vertauschung von i mit $-i$ aus $\varphi(1, p)$ hervorgeht, dass also

$$\varphi(-1, p) = (-i)^{1/4(p-1)^2} \sqrt{p}$$

ist; durch Vergleichung dieser beiden Ausdrücke, in denen $\sqrt{p}$ beide Male positiv zu nehmen ist, ergiebt sich aber

$$\left(\frac{-1}{p}\right) = (-1)^{1/4(p-1)^2} = (-1)^{1/2(p-1)}.$$

Setzen wir ferner in dem dritten Satz des §. 113

$$h = 1, \quad m = 8, \quad n = p,$$

so erhalten wir

$$\varphi(8, p)\, \varphi(p, 8) = \varphi(1, 8p);$$

nun ist aber

$$\varphi(1, 8p) = (1 + i)\sqrt{8p} = 4\sqrt{p} \,.\, e^{1/4\pi i},$$

ferner

$$\varphi(p, 8) = 4\, e^{1/4 p\pi i},$$

ferner (nach dem zweiten Satze des §. 113)

$$\varphi(8, p) = \varphi(2 \,.\, 2^2, p) = \varphi(2, p),$$

d. h.

$$\varphi(8, p) = \left(\frac{2}{p}\right) \varphi(1, p) = \left(\frac{2}{p}\right) i^{1/4(p-1)^2} \sqrt{p};$$

setzen wir diese Werthe für $\varphi(8, p)$, $\varphi(p, 8)$ und $\varphi(1, 8p)$ in die vorangehende Gleichung ein, so erhalten wir

$$\left(\frac{2}{p}\right) i^{1/4(p-1)^2} \sqrt{p} \,.\, 4\, e^{1/4 p\pi i} = 4\sqrt{p} \,.\, e^{1/4\pi i},$$

und hieraus folgt leicht

$$\left(\frac{2}{p}\right) = (-1)^{1/8(p^2-1)}.$$

Auf diese Weise sind alle Hauptsätze der Theorie der quadratischen Reste von Neuem bewiesen.

§. 116.

Für den Fall, dass p eine ungerade Primzahl, und h irgend eine durch p nicht theilbare ganze Zahl ist, haben wir im vorigen Paragraphen folgende Gleichung erhalten

$$\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) \varphi(1, p),$$

welche, wenn man den für $\varphi(1, p)$ gefundenen Werth einsetzt, in die folgende übergeht:

$$\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p}; \qquad (1)$$

soll dieselbe auch für den vorher ausgeschlossenen Fall, in welchem $h \equiv 0 \pmod{p}$ ist, ihre Gültigkeit behalten, so müssen wir übereinkommen, immer

$$\left(\frac{h}{p}\right) = 0$$

zu setzen, wenn h durch p theilbar ist; denn die linke Seite der Gleichung wird

$$\Sigma \left(\frac{s}{p}\right) = 0,$$

weil die Anzahl der quadratischen Reste genau gleich ist der Anzahl der quadratischen Nichtreste. Nach dieser Erweiterung des von Legendre eingeführten Zeichens wird ferner, wenn man an der in §. 46 gegebenen Erklärung des Jacobi'schen Symbols festhält, stets

$$\left(\frac{m}{P}\right) = 0,$$

wenn m keine relative Primzahl zu P ist.

Die Gleichung (1) gilt jetzt allgemein für jede positive ungerade Primzahl p, wenn h irgend eine ganze Zahl bedeutet, und die Summation linker Hand darf auch auf die Zahlclasse $s \equiv 0 \pmod{p}$ ausgedehnt werden. Wir wollen nun zeigen, dass dieser Satz über ungerade positive Primzahlen p sich genau in derselben Fassung

auch auf jede positive ungerade zusammengesetzte Zahl P übertragen lässt, welche durch keine Quadratzahl (ausser 1) theilbar ist. Wir setzen also

$$P = pp'p'' \dots$$

wo $p, p', p'' \dots$ lauter positive ungerade und von einander verschiedene Primzahlen bedeuten, und führen der Bequemlichkeit halber folgende Bezeichnung ein:

$$\frac{P}{p} = Q, \quad \frac{P}{p'} = Q', \quad \frac{P}{p''} = Q'' \dots$$

Schreiben wir nun für jede der Primzahlen $p, p', p'' \dots$ die obige Gleichung (1) auf:

$$\Sigma \left(\frac{s}{p}\right) e^{s\frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{1/4(p-1)^2} \sqrt{p}$$

$$\Sigma \left(\frac{s'}{p'}\right) e^{s'\frac{2h\pi i}{p'}} = \left(\frac{h}{p'}\right) i^{1/4(p'-1)^2} \sqrt{p'}$$

$$\Sigma \left(\frac{s''}{p''}\right) e^{s''\frac{2h\pi i}{p''}} = \left(\frac{h}{p''}\right) i^{1/4(p''-1)^2} \sqrt{p''}$$

$$\dots\dots\dots\dots$$

und setzen wir zur Abkürzung

$$s\,Q + s'\,Q' + s''\,Q'' + \dots = m,$$

so ergiebt, da auch nach der neuen Erweiterung des Legendre'schen Symbols stets

$$\left(\frac{h}{p}\right)\left(\frac{h}{p'}\right)\left(\frac{h}{p''}\right)\dots = \left(\frac{h}{P}\right)$$

ist, die Multiplication aller dieser Gleichungen folgendes Resultat

$$\left.\begin{array}{l} \Sigma \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right)\dots e^{m\frac{2h\pi i}{P}} \\ = \left(\frac{h}{P}\right) i^{1/4(p-1)^2 + 1/4(p'-1)^2 + 1/4(p''-1)^2 + \dots} \sqrt{P}, \end{array}\right\} \quad (2)$$

wo $\sqrt{P}$ wieder positiv zu nehmen ist, und das Summenzeichen linker Hand sich auf alle $pp'p'' \dots = P$ Combinationen aller Werthe von $s, s', s'' \dots$ bezieht. Zunächst leuchtet nun ein, dass je zwei verschiedenen dieser Combinationen auch zwei nach dem Modulus P incongruente Werthe von m entsprechen; denn aus

$$sQ + s'Q' + s''Q'' + \cdots \equiv tQ + t'Q' + t''Q'' + \cdots \pmod{P}$$

würde, da Q', Q'' ... sämmtlich $\equiv 0 \pmod{p}$ sind, folgen, dass

$$sQ \equiv tQ \pmod{p},$$

und, da Q relative Primzahl zu p ist, auch

$$s \equiv t \pmod{p}$$

wäre; ähnlich würde aus derselben Annahme gleichzeitig

$$s' \equiv t' \pmod{p'}; \quad s'' \equiv t'' \pmod{p''} \ldots$$

folgen, so dass also die beiden Combinationen $s, s', s'' \ldots$ und $t, t', t'' \ldots$ identisch wären. In der That durchläuft also m ein vollständiges Restsystem in Bezug auf den Modulus P. Ferner ist nun

$$\left(\frac{m}{p}\right) = \left(\frac{sQ + s'Q' + s''Q'' + \cdots}{p}\right) = \left(\frac{sQ}{p}\right) = \left(\frac{s}{p}\right)\left(\frac{Q}{p}\right),$$

und ebenso

$$\left(\frac{m}{p'}\right) = \left(\frac{s'}{p'}\right)\left(\frac{Q'}{p'}\right), \quad \left(\frac{m}{p''}\right) = \left(\frac{s''}{p''}\right)\left(\frac{Q''}{p''}\right) \cdots,$$

folglich auch, wenn man alle diese Gleichungen multiplicirt,

$$\left(\frac{m}{P}\right) = \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right) \cdots \left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right) \cdots$$

Multiplicirt man daher beide Seiten der obigen Gleichung (2) mit

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right) \cdots,$$

so erhält man

$$\Sigma \left(\frac{m}{P}\right) e^{m\frac{2h\pi i}{P}} = \left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right) \cdots \left(\frac{h}{P}\right) i^{\Sigma \frac{1}{4}(p-1)^2} \sqrt{P},$$

wo rechts zur Abkürzung

$$\left(\frac{p-1}{2}\right)^2 + \left(\frac{p'-1}{2}\right)^2 + \left(\frac{p''-1}{2}\right)^2 + \cdots = \Sigma \left(\frac{p-1}{2}\right)^2$$

gesetzt ist. Da nun ferner

$$\left(\frac{Q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{p''}{p}\right) \cdots$$

$$\left(\frac{Q'}{p'}\right) = \left(\frac{p}{p'}\right)\left(\frac{p''}{p'}\right) \cdots$$

$$\left(\frac{Q''}{p''}\right) = \left(\frac{p}{p''}\right)\left(\frac{p'}{p''}\right) \cdots$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

ist, so erhält man durch Multiplication

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots = \Pi\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right),$$

wo das Productzeichen Π sich auf alle möglichen Paare von je zwei verschiedenen Primzahlen p, p' bezieht. Da nun nach dem Reciprocitätssatze

$$\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)} = i^{\frac{1}{2}(p-1)(p'-1)}$$

ist, so erhält man

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots = i^{2\Sigma\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)},$$

wo das Summenzeichen rechter Hand sich wieder auf alle Combinationen von je zwei verschiedenen Primzahlen p, p' bezieht; es ist ferner

$$\Sigma\left(\frac{p-1}{2}\right)^2 + 2\,\Sigma\,\frac{p-1}{2}\,\frac{p'-1}{2}$$
$$= \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots\right)^2,$$

folglich

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right)i^{[\frac{1}{2}(p-1)+\frac{1}{2}(p'-1)+\cdots]^2}\sqrt{P}.$$

Da endlich (vergl. §. 46)

$$P = (1+(p-1))(1+(p'-1))(1+(p''-1))\ldots$$
$$\equiv 1 + (p-1) + (p'-1) + (p''-1) + \cdots \pmod{4}$$

und folglich

$$\frac{P-1}{2} \equiv \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots \pmod{2}$$

und hieraus

$$\left(\frac{P-1}{2}\right)^2 \equiv \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2}\cdots\right)^2 \pmod{4}$$

ist, so ergiebt sich schliesslich

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right)i^{\frac{1}{4}(P-1)^2}\sqrt{P},$$

worin der zu beweisende Satz besteht. Nimmt man $h \equiv 0 \pmod{P}$, so erhält man wieder den (in §. 52. I. bewiesenen) Satz

$$\Sigma\left(\frac{m}{P}\right) = 0.$$

II. Ueber den Grenzwerth einer unendlichen Reihe.

§. 117.

Lehrsatz: Sind a und b zwei positive Constanten, so convergirt die unendliche Reihe

$$S = \frac{1}{b^{1+\varrho}} + \frac{1}{(b+a)^{1+\varrho}} + \frac{1}{(b+2a)^{1+\varrho}} + \frac{1}{(b+3a)^{1+\varrho}} + \cdots$$

für jeden positiven Werth von ϱ, und bei unbegrenzter Abnahme dieser positiven Zahl ϱ nähert sich das Product ϱS dem Grenzwerthe a^{-1}.

Beweis. Construiren wir für einen bestimmten positiven Werth von ϱ die Curve, deren Gleichung in Bezug auf ein rechtwinkliges Coordinatensystem

$$y = \frac{1}{x^{1+\varrho}}$$

ist, so hat die Fläche, welche zwischen ihr und der unendlichen positiven Abscissenaxe liegt, von $x = b$ an gerechnet, den endlichen Werth

$$\int_b^{+\infty} y\,dx = \frac{1}{\varrho\, b^{\varrho}}.$$

Die Ordinaten der Curve, welche den Abscissen

$$b,\ b+a,\ b+2a,\ b+3a \ldots$$

entsprechen, sind

$$\frac{1}{b^{1+\varrho}},\ \frac{1}{(b+a)^{1+\varrho}},\ \frac{1}{(b+2a)^{1+\varrho}},\ \frac{1}{(b+3a)^{1+\varrho}}\cdots;$$

ihre Fusspuncte sind äquidistant und zerlegen die Abscissenaxe in unendlich viele Stücke von der Grösse a. Construirt man über jedem dieser Stücke als Grundlinie ein Rechteck, dessen Höhe gleich der letzten Ordinate in diesem Stück ist, so haben diese Rechtecke der Reihe nach den Flächeninhalt

$$\frac{a}{(b+a)^{1+\varrho}},\ \frac{a}{(b+2a)^{1+\varrho}},\ \frac{a}{(b+3a)^{1+\varrho}}\cdots$$

Da nun die Ordinate y der Curve mit stetig wachsendem x stetig abnimmt, so ist jedes dieser Rechtecke kleiner als der über demselben Abscissenstück liegende, bis zur Curve ausgedehnte Flächenstreifen, und folglich ist die Summe von noch so vielen jener Rechtecke stets kleiner als die gesammte, oben von der Curve begrenzte Fläche; d. h. es ist

$$\frac{a}{(b+a)^{1+\varrho}}+\frac{a}{(b+2a)^{1+\varrho}}+\frac{a}{(b+3a)^{1+\varrho}}+\cdots<\frac{1}{\varrho b^{\varrho}},$$

oder es ist, wenn auf beiden Seiten $ab^{-1-\varrho}$ addirt wird,

$$aS<\frac{1}{\varrho b^{\varrho}}+\frac{a}{b^{1+\varrho}},$$

woraus folgt, dass die aus lauter positiven Gliedern bestehende Reihe S wirklich für jeden positiven Werth von ϱ convergirt.

Construirt man nun über jedem der obigen Abscissenstücke als Grundlinie ein zweites Rechteck, dessen Höhe gleich der ersten Ordinate in diesem Stück ist, so sind diese Rechtecke, deren Flächeninhalt gleich

$$\frac{a}{b^{1+\varrho}},\ \frac{a}{(b+a)^{1+\varrho}},\ \frac{1}{(b+2a)^{1+\varrho}}\cdots,$$

nothwendig grösser als die über denselben Stücken liegenden, bis zur Curve fortgesetzten Flächenstreifen, aus dem schon oben angeführten Grunde, weil mit wachsendem x die Ordinate y stetig abnimmt. Die Summe aller dieser Rechtecke ist daher grösser als die gesammte, oben von der Curve begrenzte Fläche, d. h. es ist

$$aS>\frac{1}{\varrho b^{\varrho}}.$$

Auf diese Weise ist der Werth der unendlichen Reihe S und folglich auch der des Productes ϱS in zwei Grenzen eingeschlossen; es ist nämlich

$$\frac{1}{a\, b^{\varrho}} < \varrho\, S < \frac{1}{a\, b^{\varrho}} + \frac{\varrho}{b^{1+\varrho}}.$$

Wenn nun der positive Werth ϱ unendlich klein wird, so nähert sich sowohl

$$\frac{1}{a\, b^{\varrho}}, \text{ als auch } \frac{1}{a\, b^{\varrho}} + \frac{\varrho}{b^{1+\varrho}}$$

einem und demselben Grenzwerth a^{-1}; mithin muss auch das Product ϱS sich demselben Grenzwerth a^{-1} nähern, was zu beweisen war.

§. 118.

Der so eben bewiesene Satz bildet nur einen speciellen Fall des folgenden, welcher seiner zahlreichen Anwendungen wegen von der grössten Wichtigkeit ist:

Es sei K ein System von positiven Zahlwerthen k, und T diejenige unstetige Function von einer positiven stetigen Veränderlichen t, welche angiebt, wie viele der in K enthaltenen Zahlwerthe k den Werth t nicht übertreffen; wenn nun mit unendlich wachsendem t der Quotient $T:t$ sich einem bestimmten endlichen Grenzwerthe ω nähert, so convergirt die Reihe

$$S = \Sigma\, \frac{1}{k^{1+\varrho}}$$

für jeden positiven Werth von ϱ, und das Product $\varrho\, S$ nähert sich mit unendlich abnehmendem ϱ demselben Grenzwerthe ω.

Es wird gut sein, dem Beweise dieses allgemeinen Princips*) einige erläuternde Bemerkungen voranzuschicken. Zufolge der Bedeutung von T entspricht jedem endlichen Werthe von t auch

*) *Dirichlet: Recherches* etc. §. 1. — *Dirichlet: Sur un théorème relatif aux séries*, Crelle's Journal Bd. LIII.

ein endlicher Werth von T; denn wären in K unendlich viele Zahlen k enthalten, welche den endlichen Werth t nicht übertreffen, so würde auch jedem grössern Werthe von t eine unendliche Anzahl T entsprechen; es würde daher das Verhältniss $T:t$ fortwährend unendlich gross sein; dies widerspricht aber der Annahme, dass $T:t$ sich einem endlichen Grenzwerth ω mit wachsendem t nähert. Es leuchtet ferner ein, dass die ganze Zahl T nur dann ihren Werth ändert, wenn t einen Werth erreicht, welcher einer oder mehreren einander gleichen in K enthaltenen Zahlen k gleich ist, und zwar wird T dann plötzlich um ebenso viele Einheiten zunehmen, als es Zahlen k giebt, welche diesem Werth t gleich sind.

In dem einfachsten Falle, wenn K nur aus einer endlichen Anzahl von Zahlwerthen k besteht, leuchtet die Richtigkeit des obigen Satzes unmittelbar ein; denn sobald t dem grössten dieser Werthe k gleich geworden ist, bleibt T bei weiter wachsendem t unverändert; es ist folglich $\omega = 0$; und da andererseits die Summe

$$\Sigma \frac{1}{k}$$

einen endlichen Werth hat, so wird auch das Product ϱS mit unendlich kleinem ϱ ebenfalls unendlich klein werden.

Ebenso bestätigt sich der allgemeine Satz in dem speciellen Falle, welcher in dem vorigen Paragraphen behandelt ist. Das System K besteht dort aus den sämmtlichen Zahlen von der Form $b + na$, die den sämmtlichen Werthen $0, 1, 2, 3 \ldots$ von n entsprechen; wenn nun $t = b + na$ oder $> b + na$, aber $< b + (n+1)a$ ist, so ist entsprechend $T = n + 1$, und folglich nähert sich der Quotient $T:t$ mit unendlich wachsendem t, also auch mit unendlich wachsendem n dem Grenzwerth

$$\omega = \frac{1}{a};$$

und in der That haben wir gefunden, dass dieser Werth auch zugleich der Grenzwerth des Productes ϱS ist, wenn die positive Grösse ϱ unendlich klein wird.

§. 119.

Wir gehen nun zu dem Beweise des allgemeinen Satzes über und beginnen damit, die in K enthaltenen Zahlwerthe k ihrer Grösse nach zu ordnen und mit Indices zu versehen, in der Weise, dass

$$k_1 \leqq k_2 \leqq k_3 \leqq k_4 \leqq k_5 \ldots$$

wird; dies ist offenbar möglich, da unterhalb eines beliebigen endlichen positiven Werthes t immer nur eine endliche Anzahl von Zahlwerthen k vorhanden ist; sind mehrere Zahlen k gleich gross, so muss jede einzelne ihren besondern Index erhalten, so dass dann mehreren auf einander folgenden Indices gleich grosse Zahlwerthe k entsprechen.

Sehen wir ab von dem interesselosen Falle, in welchem nur eine endliche Anzahl von Werthen k vorhanden ist, so lässt sich zunächst zeigen, dass mit unbegrenzt wachsendem n auch der Quotient

$$h_n = \frac{n}{k_n}$$

sich demselben Grenzwerth ω nähert, und durch diese Bemerkung wird dann der allgemeine Satz auf den vorher (§. 117) behandelten speciellen Fall zurückgeführt.

In der That, wenn δ eine beliebig kleine positive gegebene Grösse bedeutet, so kann man entsprechend einen positiven Werth τ immer so gross wählen, dass für alle Werthe $t \geqq \tau$ die Bedingung

$$\omega - \delta < \frac{T}{t} < \omega + \delta$$

erfüllt ist. Es sei ferner ν derjenige Werth von T, welcher $t = \tau$ entspricht, also $k_\nu \leqq \tau < k_{\nu+1}$, und n irgend eine der positiven ganzen Zahlen $\nu + 1$, $\nu + 2$, $\nu + 3 \ldots$; dann ist jedenfalls $k_n > \tau$, und wenn mehrere auf einander folgende Grössen k denselben Werth wie k_n besitzen, so sei k_{m+1} die erste, k_r die letzte von ihnen, also n eine der Zahlen $m + 1$, $m + 2 \ldots r$. Nähert sich nun t von k_m ab wachsend dem Werthe k_n immer mehr an, so bleibt $T = m$, und der Quotient $T : t$ nähert sich abnehmend unbegrenzt dem Werthe $m : k_n$, und da $m < n$ ist, so folgt, dass

$$\frac{T}{t} < h_n$$

ist, sobald t sehr nahe unterhalb k_n liegt; für $t = k_n$ wird aber $T = r \geqq n$, und folglich

$$\frac{T}{t} \geqq h_n.$$

Da nun bei diesem Wachsen von $t < k_n$ bis $t = k_n > \tau$ der Quotient $T:t$ stets zwischen $\omega - \delta$ und $\omega + \delta$ liegt, und zugleich, wie eben gezeigt ist, von Werthen, die $< h_n$ sind, auf einen Werth springt, der $\geqq h_n$ ist, so muss auch $\omega - \delta < h_n < \omega + \delta$ sein. Wie klein also auch δ sein mag, so kann n stets so gross gewählt werden, dass h_n definitiv um weniger als δ von ω verschieden wird, d. h. h_n nähert sich mit unbegrenzt wachsendem n demselben Grenzwerth ω.

Mit Hülfe dieses Resultates lässt sich der Beweis des allgemeinen Satzes leicht führen. Da nämlich

$$S = \Sigma \frac{1}{k^{1+\varrho}} = \frac{h_1^{1+\varrho}}{1^{1+\varrho}} + \frac{h_2^{1+\varrho}}{2^{1+\varrho}} + \frac{h_3^{1+\varrho}}{3^{1+\varrho}} + \cdots$$

ist, wo h_n mit unendlich wachsendem n sich dem Grenzwerthe ω nähert und folglich endlich, d. h. kleiner als eine angebbare Constante H bleibt, so ist die Summe S' der ersten n Glieder der Reihe S kleiner als das Product aus $H^{1+\varrho}$ und der Summe $\mathfrak{S}'$ der ersten n Glieder der folgenden Reihe

$$\mathfrak{S} = \frac{1}{1^{1+\varrho}} + \frac{1}{2^{1+\varrho}} + \frac{1}{3^{1+\varrho}} + \cdots;$$

da nun die letztere (nach §. 117) für jeden *positiven* Werth von ϱ convergirt, so *convergirt* auch die Reihe S. Setzt man nun $S = S' + S''$, $\mathfrak{S} = \mathfrak{S}' + \mathfrak{S}''$, so wird $S'' = h^{1+\varrho}\,\mathfrak{S}''$, wo h einen (jedenfalls positiven) Mittelwerth aus den Werthen $h_{n+1}, h_{n+2} \ldots$ bedeutet. Ist daher δ eine beliebig kleine positive gegebene Grösse, und n so gross gewählt (was stets möglich ist), dass alle diese Werthe zwischen $\omega - \delta$ und $\omega + \delta$ liegen, so wird auch h, und für hinreichend kleine Werthe von ϱ auch $h^{1+\varrho}$ zwischen denselben Grenzen liegen. Da ferner (nach §. 117) das Product $\varrho\,\mathfrak{S}''$ mit unbegrenzt abnehmendem positiven ϱ sich der Einheit unendlich annähert, so wird für hinreichend kleine Werthe von ϱ auch das Product $\varrho S'' = h^{1+\varrho} . \varrho\mathfrak{S}''$ zwischen den Grenzen $\omega - \delta$ und $\omega + \delta$ liegen. Da endlich $\varrho S'$ gleichzeitig unendlich klein wird, weil S' nur

eine endliche Anzahl von Gliedern enthält, so wird für sehr kleine Werthe von ϱ auch $\varrho S = \varrho S' + \varrho S''$ zwischen denselben Grenzen $\omega - \delta$ und $\omega + \delta$ liegen. Hiermit ist also auch bewiesen, dass mit unbegrenzt abnehmendem ϱ das Product ϱS *sich dem Grenzwerthe* ω *unendlich annähert**).

*) Es verdient bemerkt zu werden, dass man den obigen allgemeinen Satz nicht umkehren darf. Besteht z. B. das System K aus einer Zahl $k = 1$, aus $(\theta - 1)$ Zahlen $k = \theta$, aus $(\theta^2 - \theta)$ Zahlen $k = \theta^2$, aus $(\theta^3 - \theta^2)$ Zahlen $k = \theta^3$ u. s. f., wo θ eine positive ganze Zahl > 1 bedeutet, so ist für jeden positiven Werth von ϱ

$$S = 1 + \frac{\theta - 1}{\theta(\theta^\varrho - 1)},$$

und das Product ϱS nähert sich mit unendlich abnehmendem ϱ dem Grenzwerthe

$$\omega = \frac{\theta - 1}{\theta \log \theta},$$

während der Quotient $T : t$ bei unendlich wachsendem t fortwährend von dem Werth 1 abnehmend durch ω hindurch geht bis zu dem Werth $1 : \theta$, dann aber sogleich wieder zu dem Werth 1 zurückspringt, um von Neuem denselben Veränderungsprocess zu erleiden (vergl. §. 144).

III. Ueber einen geometrischen Satz.

§. 120.

In einer Ebene sei eine vollständig begrenzte Figur F von allenthalben endlichen Dimensionen construirt, deren Flächeninhalt wir mit A bezeichnen wollen. Sind ferner X und Y zwei auf einander senkrechte Axen, und construirt man parallel mit ihnen zwei Systeme äquidistanter Parallelen, welche ein über die ganze Ebene ausgebreitetes Gitter bilden, so wird, wenn δ der Abstand je zweier benachbarter Parallelen, und T die Anzahl der Gitterpuncte ist, welche innerhalb F liegen, das Product $T\delta^2$ mit unendlich abnehmendem δ sich dem Grenzwerthe A nähern*).

Um diesen Satz zu beweisen, betrachten wir das System der mit Y parallelen Geraden und nehmen der Einfachheit halber an, dass jede derselben die Begrenzung der Figur nur zweimal schneidet; bezeichnen wir mit h die Länge des innerhalb F liegenden Stückes irgend einer solchen Parallelen, so ist $h\delta$ nahezu der Flächeninhalt des zwischen dieser und der folgenden Parallelen enthaltenen Theiles der Fläche F, und es wird in der Lehre von der Quadratur bewiesen, dass die Summe aller dieser Rechtecke $h\delta$ sich mit unendlich abnehmendem δ dem wahren Flächeninhalt A der Figur unbegrenzt nähert. Bezeichnen wir nun mit n die Anzahl der auf h liegenden Gitterpuncte (wobei es gleichgültig ist, ob ein zufällig auf der Begrenzung von F liegender Gitterpunct mitgezählt oder ausgeschlossen wird), so besteht h aus $(n-1)$ Stücken $= \delta$ und aus einem Rest, welcher höchstens $= 2\delta$ ist,

*) *Dirichlet: Recherches* etc. §. 1.

so dass wir $h = n\delta + \varepsilon\delta$ setzen können, wo ε einen positiven oder negativen echten Bruch bedeutet. Es ist daher

$$\sum h\delta = \sum (n\delta^2 + \varepsilon\delta^2) = T\delta^2 + \delta \sum \varepsilon\delta;$$

es ist ferner, da ε absolut genommen höchstens $= 1$ ist, die Summe $\sum \varepsilon\delta$ höchstens gleich der endlichen Ausdehnung der Figur F in der Richtung der Axe X, und es wird daher $\delta \sum \varepsilon\delta$ mit δ gleichzeitig unendlich klein. Folglich nähert sich das Product $T\delta^2$ demselben Grenzwerthe A, welchem sich $\sum h\delta$ nähert; was zu beweisen war.

Es leuchtet übrigens ein, dass dieser Satz nicht an die Beschränkung gebunden ist, nach welcher die Parallelen mit der Axe Y nur einmal in die Figur F ein- und nur einmal aus ihr austreten. Man kann immer die Figur F als ein Aggregat von positiven und negativen Flächentheilen ansehen, welche einzeln der angegebenen Bedingung genügen; und wendet man auf jeden einzelnen Theil den Satz an, so ergiebt sich daraus sofort die Richtigkeit desselben für die ganze Figur F.

IV. Ueber die Geschlechter, in welche die Classen der quadratischen Formen von bestimmter Determinante zerfallen *).

§. 121.

Ist (a, b, c) eine quadratische Form von der Determinante $b^2 - ac = D$, und sind z, z' irgend zwei durch diese Form darstellbare Zahlen (wobei es gleichgültig ist, ob die darstellenden Zahlen relative Primzahlen sind oder nicht), so lässt sich das Product zz' stets in die Form $x^2 - Dy^2$ bringen, wo x und y ganze Zahlen bedeuten; denn aus der Annahme

$$z = a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \quad z' = a\beta^2 + 2b\beta\delta + c\delta^2$$

folgt (nach §. 54), dass die Form (a, b, c) durch die Substitution $\binom{\alpha,\ \beta}{\gamma,\ \delta}$ in eine Form (z, x, z') übergeht, deren Determinante $x^2 - zz'$ von der Form Dy^2 ist. Aus dieser Bemerkung lassen sich folgende Schlüsse ziehen **).

1. Ist l eine ungerade in D aufgehende Primzahl, so hat für alle durch l nicht theilbaren Zahlen n, welche durch die Form (a, b, c) darstellbar sind, das Symbol

$$\left(\frac{n}{l}\right)$$

einen und denselben Werth. Denn sind n und n' irgend zwei solche durch l nicht theilbare und durch (a, b, c) darstellbare

*) *Dirichlet: Recherches sur diverses applications* etc. §§. 3, 6 (Crelle's Journal XIX).

**) Vergl. *Gauss: D. A.* artt. 229—231.

Zahlen, so folgt aus $nn' = x^2 - Dy^2$, dass $nn' \equiv x^2 \pmod{l}$, und folglich

$$\left(\frac{nn'}{l}\right) = +1, \quad \text{also} \quad \left(\frac{n}{l}\right) = \left(\frac{n'}{l}\right)$$

ist.

2. Ist $D \equiv 3 \pmod{4}$, so hat für alle ungeraden durch die Form darstellbaren Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)}$$

einen und denselben Werth. Denn sind n und n' irgend zwei solche ungerade Zahlen, so ist

$$nn' = x^2 - Dy^2 \equiv x^2 + y^2 \pmod{4};$$

da ferner nn' eine ungerade Zahl ist, so muss eine der beiden Zahlen x, y gerade, die andere ungerade sein; hieraus folgt $nn' \equiv 1 \pmod{4}$, also auch $n \equiv n' \pmod{4}$, und hieraus

$$(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(n'-1)}.$$

3. Ist $D \equiv 2 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{8}(n^2-1)}$$

einen und denselben Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 - 2y^2 \pmod{8}$$

folgt, da x ungerade ist, $nn' \equiv \pm 1 \pmod{8}$, also auch $n \equiv \pm n' \pmod{8}$, woraus die obige Behauptung sich unmittelbar ergiebt.

4. Ist $D \equiv 6 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}$$

einen und denselben Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 + 2y^2 \pmod{8}$$

folgt, da x ungerade ist, $nn' \equiv 1$ oder $\equiv 3 \pmod{8}$, je nachdem y gerade oder ungerade ist; dann ist entsprechend $n \equiv n'$ oder $\equiv 3n' \pmod{8}$, und man findet leicht, dass in beiden Fällen

$$\frac{n-1}{2} + \frac{n^2-1}{8} \equiv \frac{n'-1}{2} + \frac{n'^2-1}{8} \pmod{2}$$

ist, was zu beweisen war.

5. Ist $D \equiv 4 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n der Ausdruck

$$(-1)^{\frac{1}{2}(n-1)}$$

einen und denselben Werth. Denn aus $nn' = x^2 - Dy^2$ folgt, da x ungerade ist, $nn' \equiv 1 \pmod{4}$, also $n \equiv n' \pmod{4}$.

6. Ist $D \equiv 0 \pmod{8}$, so hat für alle durch dieselbe Form darstellbaren ungeraden Zahlen n jeder der beiden Ausdrücke

$$(-1)^{\frac{1}{2}(n-1)} \text{ und } (-1)^{\frac{1}{8}(n^2-1)}$$

für sich einen unveränderlichen Werth. Denn aus

$$nn' = x^2 - Dy^2 \equiv x^2 \equiv 1 \pmod{8}$$

folgt $n \equiv n' \pmod{8}$.

§. 122.

Auf den Sätzen des vorigen Paragraphen beruht die Eintheilung der quadratischen Formen einer gegebenen Determinante D in *Geschlechter*; wir beschränken uns hier auf die *ursprünglichen* Formen, weil das, was für sie gilt, leicht auf die anderen Formen übertragen werden kann; ausserdem betrachten wir für den Fall einer negativen Determinante nur *positive*, d. h. solche Formen, deren äussere Coefficienten positiv sind. Es sei also (a, b, c) eine ursprüngliche Form der σten Art (§. 61), so wissen wir (§. 93), dass man den Variabeln derselben stets solche Werthe x, y beilegen kann, dass

$$\frac{ax^2 + 2bxy + cy^2}{\sigma} = n$$

positiv und relative Primzahl zu $2D$ wird; dabei ist es gleichgültig, ob x und y relative Primzahlen zu einander sind oder nicht. Bezeichnet man nun mit $l, l', l'' \ldots$ alle von einander verschiedenen in D aufgehenden ungeraden Primzahlen, so hat für alle durch eine und dieselbe Form (a, b, c) erzeugten Zahlen σn jedes der Symbole

$$\left(\frac{\sigma n}{l}\right), \left(\frac{\sigma n}{l'}\right), \left(\frac{\sigma n}{l''}\right) \ldots$$

und folglich auch jedes der Symbole

$$\left(\frac{n}{l}\right), \left(\frac{n}{l'}\right), \left(\frac{n}{l''}\right) \ldots$$

für sich einen unveränderlichen Werth; ist ferner D nicht $\equiv 1$ (mod. 4), also $\sigma = 1$, so gilt dasselbe, je nachdem $D \equiv 3$ (mod. 4), $D \equiv 2$ (mod. 8), $D \equiv 6$ (mod. 8), $D \equiv 4$ (mod. 8), $D \equiv 0$ (mod. 8) ist, entsprechend von dem Ausdruck

$$(-1)^{\frac{1}{2}(n-1)}, \quad (-1)^{\frac{1}{8}(n^2-1)}, \quad (-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)}, \quad (-1)^{\frac{1}{2}(n-1)}$$

oder von jedem der beiden Ausdrücke

$$(-1)^{\frac{1}{2}(n-1)} \text{ und } (-1)^{\frac{1}{8}(n^2-1)}.$$

Die Anzahl dieser Ausdrücke

$$\left(\frac{n}{l}\right), \left(\frac{n}{l'}\right) \cdots (-1)^{\frac{1}{2}(n-1)} \text{ u. s. w.},$$

die wir die *Charaktere* C nennen wollen, hängt nur von der Determinante D ab und soll im Folgenden immer mit λ bezeichnet werden; offenbar ist λ gleich der Anzahl der in D aufgehenden ungeraden Primzahlen $l, l', l'' \ldots$, wenn $D \equiv 1$ (mod. 4); in den übrigen Fällen mit Ausnahme von $D \equiv 0$ (mod. 8) ist sie um 1 und im Falle $D \equiv 0$ (mod. 8) ist sie um 2 grösser. Das System der bestimmten Werthe ± 1, welche diesen λ Charakteren C für eine bestimmte Form (a, b, c) zukommen, wollen wir den *Total-Charakter* dieser Form nennen. Nach dem Ausfall dieses Total-Charakters theilen wir sämmtliche ursprüngliche Formen von gleicher Determinante und gleicher Art in *Geschlechter* ein, indem wir je zwei Formen in dasselbe Geschlecht oder in zwei verschiedene Geschlechter werfen, je nachdem der Total-Charakter der einen Form mit dem der andern identisch ist, oder nicht; ein Geschlecht ist hiernach der Inbegriff aller ursprünglichen Formen von gleicher Determinante und gleicher Art, für welche jeder der λ Charaktere C für sich genommen denselben Werth besitzt. Da nun alle Zahlen σn, welche durch eine bestimmte Form darstellbar sind, auch durch alle mit ihr äquivalenten Formen dargestellt werden können, so gehören alle Formen einer und derselben *Classe* auch in ein und dasselbe *Geschlecht*; ein Geschlecht ist daher immer der Inbegriff einer bestimmten Anzahl von Formen-Classen. Da ferner jeder der λ Charaktere C zwei einander entgegengesetzte Werthe haben kann, so leuchtet ein, dass die sämmtlichen ursprünglichen Formen von einer gegebenen Determinante D und von der σten Art *höchstens* 2^λ verschiedene Genera bilden können.

Wir bemerken nun noch, dass die äussern Coefficienten einer Form immer durch diese Form dargestellt werden, wenn man der

einen Variabeln den Werth 1, der andern den Werth 0 beilegt; mithin können die Charaktere dieser Form immer aus einem dieser beiden Coefficienten erkannt werden.

Beispiel 1: Für die Determinante $D = -35 \equiv 1 \pmod 4$ bilden (§. 67) die sechs Formen

$$(1, 0, 35), \quad (5, 0, 7), \quad (3, \pm 1, 12), \quad (4, \pm 1, 9)$$

ein vollständiges System nicht äquivalenter (positiver) Formen der ersten Art, und die beiden Formen

$$(2, 1, 18), \quad (6, 1, 6)$$

ein solches Formensystem der zweiten Art. Um diese Formen (oder die durch sie repräsentirten Classen) in Geschlechter einzutheilen, haben wir die beiden Charaktere

$$\left(\frac{n}{5}\right) \quad \text{und} \quad \left(\frac{n}{7}\right)$$

zu betrachten, und da $\lambda = 2$ ist, so sind für jede der beiden Formenarten *höchstens vier* Geschlechter zu erwarten. Die wirkliche Untersuchung ergiebt als Resultat folgende Tabelle

(a, b, c)	$\left(\frac{n}{5}\right)$	$\left(\frac{n}{7}\right)$
(1, 0, 35)	+	+
(5, 0, 7)	—	—
(3, ±1, 12)	—	—
(4, ±1, 9)	+	+
(2, 1, 18)	+	+
(6, 1, 6)	—	—

Es zeigt sich also, dass jedes der beiden Systeme nur in *zwei* verschiedene Geschlechter zerfällt; die drei Formen

$$(1, 0, 35), \quad (4, \pm 1, 9)$$

bilden ein Geschlecht, dessen Total-Charakter durch

$$\left(\frac{n}{5}\right) = +1, \quad \left(\frac{n}{7}\right) = +1$$

bestimmt ist; die drei anderen Formen

$$(5, 0, 7), \quad (3, \pm 1, 12)$$

bilden ein zweites Geschlecht, dessen Total-Charakter durch

$$\left(\frac{n}{5}\right) = -1, \quad \left(\frac{n}{7}\right) = -1$$

bestimmt ist. Und jede der beiden Formen der zweiten Art bildet ein Geschlecht für sich.

Beispiel 2: Für die Determinante $D = -5 \equiv 3 \pmod{4}$ bilden (§. 71) die beiden Formen

$$(1, 0, 5), \quad (2, 1, 3)$$

ein vollständiges System nicht äquivalenter (positiver) Formen; um sie in Geschlechter einzutheilen, müssen wir die beiden Charaktere

$$(-1)^{\frac{1}{2}(n-1)} \text{ und } \left(\frac{n}{5}\right)$$

betrachten. Der Form (1, 0, 5) entspricht

$$(-1)^{\frac{1}{2}(n-1)} = +1, \quad \left(\frac{n}{5}\right) = +1,$$

und der Form (2, 1, 3) entspricht

$$(-1)^{\frac{1}{2}(n-1)} = -1, \quad \left(\frac{n}{5}\right) = -1.$$

Jede dieser beiden Formen bildet also ein Geschlecht für sich; da $\lambda = 2$ ist, so ist auch hier die Anzahl der Geschlechter nicht $= 2^\lambda$, sondern nur $= 2^{\lambda-1}$.

Beispiel 3: Für die Determinante $D = 24 \equiv 0 \pmod{8}$ findet man leicht (nach §§. 75, 78, 82), dass folgende vier Formen

$$(1, 4, -8), \quad (-1, 4, 8), \quad (3, 3, -5), \quad (-3, 3, 5)$$

ein vollständiges Formensystem bilden; es sind hier die folgenden drei Charaktere zu betrachten:

$$(-1)^{\frac{1}{2}(n-1)}, \quad (-1)^{\frac{1}{8}(n^2-1)}, \quad \left(\frac{n}{3}\right);$$

der ersten der obigen Formen entspricht

$$(-1)^{\frac{1}{2}(n-1)} = +1, \quad (-1)^{\frac{1}{8}(n^2-1)} = +1, \quad \left(\frac{n}{3}\right) = +1;$$

der zweiten

$$(-1)^{\frac{1}{2}(n-1)} = -1, \quad (-1)^{\frac{1}{8}(n^2-1)} = +1, \quad \left(\frac{n}{3}\right) = -1;$$

der dritten

$$(-1)^{\frac{1}{2}(n-1)} = -1, \quad (-1)^{\frac{1}{8}(n^2-1)} = -1, \quad \left(\frac{n}{3}\right) = +1;$$

und der vierten

$$(-1)^{\frac{1}{2}(n-1)} = +1, \quad (-1)^{\frac{1}{8}(n^2-1)} = -1, \quad \left(\frac{n}{3}\right) = -1.$$

Auch hier zeigt sich also, dass die Anzahl der wirklich vorhandenen Geschlechter nicht $= 2^\lambda$, sondern nur $= 2^{\lambda-1}$ ist.

§. 123.

Mit Hülfe des Reciprocitätssatzes lässt sich nun in der That nachweisen, dass die Anzahl der verschiedenen Geschlechter *höchstens* $= 2^{\lambda-1}$ ist. Wir setzen $D = D'S^2$, wo S^2 das grösste in D aufgehende Quadrat bezeichnet, und legen den Buchstaben δ, ε, P dieselbe Bedeutung in Bezug auf D' bei, welche sie in §. 52 in Bezug auf die dort mit D bezeichnete Zahl erhalten haben. Dann wird

$$\left(\frac{D}{n}\right) = \left(\frac{D'}{n}\right) = \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right),$$

wo n jede beliebige positive ganze Zahl bedeutet, die relative Primzahl zu $2D$ ist. Da nun die Determinante D keine Quadratzahl, also D' nicht $= 1$ ist, so kann auch nicht gleichzeitig $\delta = +1$, $\varepsilon = +1$ und $P = 1$ sein, und hieraus folgt leicht, dass der Ausdruck

$$\delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P}\right)$$

entweder mit einem der Charaktere C, oder mit dem Producte aus mehreren dieser Charaktere identisch ist; bezeichnen wir diese Charaktere mit C' und ihr Product mit $\Pi\, C'$, so ist also stets

$$\Pi\, C' = \left(\frac{D}{n}\right),$$

sobald n positiv und relative Primzahl zu $2D$ ist. Da nun durch jede ursprüngliche Form der σten Art stets Zahlen σn dargestellt werden können, in welchen n dieser Bedingung genügt (§. 93), und zwar solche Zahlen σn, von welchen D quadratischer Rest ist

(§. 60), so ergiebt sich, dass der Total-Charakter einer jeden Form so beschaffen ist, dass stets

$$\Pi C' = +1$$

und niemals $\Pi C' = -1$ wird. Da nun unter den sämmtlichen 2^λ Zeichencombinationen, welche man erhält, wenn man jedem der λ Charaktere C sowohl den Werth $+1$ wie den Werth -1 beilegt, offenbar die Hälfte so beschaffen ist, dass $\Pi C' = -1$ wird, so folgt, dass diesen Zeichencombinationen oder Total-Charakteren keine wirklich existirenden Formen entsprechen können. Mithin ist die Anzahl der wirklich existirenden Geschlechter *höchstens* $= 2^{\lambda-1}$.

Im Folgenden soll nun bewiesen werden, dass allen denjenigen Total-Charakteren, welche in Uebereinstimmung mit der oben angegebenen Relation sind, wirklich existirende Formen entsprechen, dass also die Anzahl der wirklich vorhandenen Geschlechter $= 2^{\lambda-1}$ ist, und ausserdem, dass jedes Geschlecht eine gleiche Anzahl von Formen-Classen enthält.

§. 124.

Wir wollen wieder (wie in §. 89) mit n alle positiven ganzen Zahlen bezeichnen, die relative Primzahlen zu $2D$ sind, ferner mit m alle diejenigen Zahlen n, von welchen D quadratischer Rest ist, und mit μ die Anzahl der von einander verschiedenen in m aufgehenden Primzahlen. Es sei ferner $\psi(n)$ eine der Bedingung $\psi(n')\,\psi(n'') = \psi(n'n'')$ genügende Function, so ist stets

$$\Sigma\ \psi(n^2)\ \Sigma\ 2^\mu \psi(m) = \Sigma\ \psi(n)\ \Sigma\left(\frac{D}{n}\right)\psi(n),$$

vorausgesetzt, dass die hier vorkommenden unendlichen Reihen bestimmte von der Anordnung der Glieder unabhängige Werthe haben. Offenbar geht diese Gleichung durch die Specialisirung $\psi(n) = n^{-s}$ in die Endgleichung des §. 89 über, und sie könnte auch genau auf dieselbe Art wie diese bewiesen werden. Wir ziehen hier folgende Verification vor.

Verfährt man, wie in §. 91, so erhält man durch Ausführung der Multiplication der beiden unendlichen Reihen auf der rechten Seite

$$\Sigma\, \tau_n \psi(n),$$

wo

$$\tau_n = \Sigma \left(\frac{D}{\delta}\right)$$

ist, und δ alle Divisoren der Zahl n durchlaufen muss. Denkt man sich nun die Zahl n dargestellt als Product von Primzahlpotenzen $A, B \ldots$ und bezeichnet man mit a alle Divisoren von A, mit b alle Divisoren von B u. s. w., so leuchtet ein, dass τ_n das Product aus den Summen

$$\Sigma \left(\frac{D}{a}\right), \quad \Sigma \left(\frac{D}{b}\right) \cdots$$

ist. Wenn nun z. B. $A = q^\alpha$, und q eine Primzahl ist, so wird

$$\Sigma \left(\frac{D}{a}\right) = \alpha + 1,$$

wenn D quadratischer Rest von q ist; ist dagegen D Nichtrest von q, so wird

$$\Sigma \left(\frac{D}{a}\right) = 1 \quad \text{oder} \quad = 0,$$

je nachdem α gerade oder ungerade, d. h. je nachdem A ein Quadrat oder kein Quadrat ist. Bezeichnet man daher mit k alle diejenigen Zahlen n, in welchen nur solche Primfactoren aufgehen, von denen D Nichtrest ist, so folgt hieraus, dass jede Zahl n, für welche τ_n von Null verschieden ausfällt, von der Form mk^2 ist; und zwar ist dann τ_n gleich der Anzahl τ_m aller Divisoren von m. Da ferner $\psi(mk^2) = \psi(m)\psi(k^2)$ ist, so wird die rechte Seite unserer Gleichung gleich

$$\Sigma\, \tau_m \psi(mk^2) = \Sigma\, \psi(k^2) \,.\, \Sigma\, \tau_m \psi(m).$$

Wir wenden uns nun zur linken Seite; da jede Zahl n von der Form km ist, so ergiebt sich zunächst

$$\Sigma\, \psi(n^2) = \Sigma\, \psi(k^2) \,.\, \Sigma\, \psi(m^2),$$

und folglich braucht nur noch gezeigt zu werden, dass

$$\Sigma\, \psi(m^2)\, \Sigma\, 2^\mu \psi(m) = \Sigma\, \tau_m \psi(m)$$

ist*). Führen wir links die Multiplication aus, indem wir alle Glieder des Productes, welche denselben Factor $\psi(m)$ enthalten, in ein einziges zusammenfassen, so erhalten wir ein Resultat von der Form

$$\Sigma\, \tau'_m \psi(m),$$

*) Der gemeinschaftliche Werth beider Seiten ist das Quadrat von $\Sigma\, \psi(m)$.

wo der Coefficient

$$\tau'_m = \sum 2^\nu$$

aus ebenso vielen Gliedern besteht, als die Zahl m quadratische Divisoren δ^2 besitzt, und wo die Zahl ν für jede Zerlegung von der Form $m = \varepsilon\delta^2$ angiebt, wie viele verschiedene Primzahlen in ε aufgehen. Es braucht daher jetzt nur noch nachgewiesen zu werden, dass $\tau'_m = \tau_m$ ist, d. h. es muss folgender Satz bewiesen werden:

Zerlegt man eine ganze positive Zahl m auf alle mögliche Arten in zwei Factoren, von denen der eine ein Quadrat δ^2 ist, und bezeichnet man mit ν jedesmal die Anzahl der in dem andern Factor ε aufgehenden von einander verschiedenen Primzahlen, so ist $\sum 2^\nu$ gleich der Anzahl τ_m aller Divisoren der Zahl m.

Von der Richtigkeit dieses Satzes überzeugt man sich aber leicht auf folgende Weise. Ist

$$m = a^\alpha b^\beta c^\gamma \ldots,$$

wo $a, b, c \ldots$ von einander verschiedene Primzahlen bedeuten, so ist jeder Divisor ε von der Form

$$\varepsilon = ABC \ldots,$$

wo $A, B, C \ldots$ resp. irgend welche Glieder aus den Reihen

$$\begin{matrix} a^\alpha, & a^{\alpha-2}, & a^{\alpha-4} \ldots \\ b^\beta, & b^{\beta-2}, & b^{\beta-4} \ldots \\ c^\gamma, & c^{\gamma-2}, & c^{\gamma-4} \ldots \end{matrix}$$

u. s. w. bedeuten, welche so weit fortzusetzen sind, als die Exponenten nicht negativ werden. Lässt man nun jedem Factor $A, B, C \ldots$ resp. einen Factor $A', B', C' \ldots$ entsprechen, welcher $= 2$ oder $= 1$ ist, je nachdem der entsprechende Exponent > 0 oder $= 0$ ist, so wird

$$2^\nu = A'B'C' \ldots,$$

und folglich

$$\sum 2^\nu = \sum A' \,.\, \sum B' \,.\, \sum C' \ldots;$$

da aber, wie unmittelbar einleuchtet

$$\sum A' = \alpha + 1, \quad \sum B' = \beta + 1, \quad \sum C' = \gamma + 1 \ldots$$

ist, so findet man

$$\sum 2^\nu = (\alpha + 1)(\beta + 1)(\gamma + 1) \ldots = \tau_m,$$

was zu beweisen war.

Die Richtigkeit der obigen Gleichung ist also hiermit ebenfalls erwiesen.

Bei einer aufmerksamen Prüfung der vorstehenden Ableitung wird man leicht den Zusammenhang zwischen ihr und dem (in §. 91 aufgestellten) Satze über die sämmtlichen Darstellungen einer Zahl σn durch das vollständige System S der ursprünglichen Formen der σten Art erkennen, und man wird auf diese Weise zu einem sehr einfachen Beweise dieses letztern Satzes gelangen, wenn man von dem in §. 60 oder §. 86 gewonnenen Resultat ausgeht, dass die Anzahl der verschiedenen *Gruppen* von *eigentlichen* Darstellungen einer Zahl σm durch die Formen des Systems S gleich 2^μ ist, wo μ die Anzahl der verschiedenen in m aufgehenden Primzahlen bedeutet.

Schliesslich bemerken wir, dass der Satz sich bedeutend verallgemeinern lässt, wenn man statt des in ihm vorkommenden Jacobi'schen Symbols irgend eine Function $\theta(n)$ einführt, welche der Bedingung $\theta(n')\,\theta(n'') = \theta(n'n'')$ genügt und nur eine *endliche* Anzahl verschiedener Werthe besitzt.

§. 125.

Nach §. 123 zerfallen die sämmtlichen (positiven) Formen von der Determinante D und von der σten Art, und also auch die sämmtlichen h Formenclassen in höchstens $\tau = 2^{\lambda-1}$ verschiedene Geschlechter, deren Total-Charaktere sämmtlich der Bedingung

$$\Pi\, C' = +1$$

genügen, und die wir mit

$$G_1,\ G_2 \ldots G_\tau$$

bezeichnen wollen; die Anzahl der Formen-Classen, welche diese Geschlechter enthalten, sollen entsprechend mit

$$g_1,\ g_2 \ldots g_\tau$$

bezeichnet werden, so dass also, wenn eins dieser Geschlechter, z. B. G_r, nicht wirklich vorhanden sein sollte, $g_r = 0$ zu setzen ist. Es soll nun gerade im Folgenden gezeigt werden, dass dies niemals eintritt, dass also diese τ Geschlechter wirklich existiren, und ausserdem, dass sie alle gleich viele Formen-Classen enthalten, dass also

$$g_1 = g_2 = g_3 \cdots = \frac{1}{\tau}\, h$$

ist.

Zu diesem Zweck benutzen wir die im vorigen Paragraphen bewiesene Gleichung*), indem wir

$$\psi(n) = \frac{\chi(n)}{n^s}$$

setzen, wo $\chi(n)$ irgend eins der $2^\lambda = 2\tau$ Glieder der Summe bedeutet, welche durch die Entwicklung des über alle λ Charaktere C erstreckten Productes

$$\Pi(1 + C)$$

entsteht; der Bedingung $\psi(n)\,\psi(n') = \psi(nn')$ geschieht offenbar durch jede solche Specialisirung Genüge, denn alle Factoren C, aus denen eine solche Function $\chi(n)$ zusammengesetzt ist, genügen derselben Bedingung. Da ausserdem $\chi(n)$ für jede Zahl n, die relative Primzahl zu $2D$ ist, $= \pm 1$ ist, so convergiren die vier in der Gleichung vorkommenden unendlichen Reihen unabhängig von der Anordnung ihrer Glieder für jeden positiven Werth $s > 1$. Es ist also unter dieser Annahme, da $\chi(n^2) = \chi(n)\,\chi(n) = +1$ ist,

$$\Sigma \frac{1}{n^{2s}} \, \Sigma\, \chi(m) \frac{2^\mu}{m^s} = \Sigma \frac{\chi(n)}{n^s} \, \Sigma \left(\frac{D}{n}\right) \frac{\chi(n)}{n^s}.$$

Denken wir uns nun wieder (wie in §. 88) ein vollständiges System S von h Formen

$$(a, b, c), \ (a', b', c') \dots$$

von der Determinante D und von der σten Art aufgeschrieben, und unterwerfen wir die Variabeln x, y jeder Form den dort angegebenen Bedingungen I., II., III., so wird jede Zahl σm im Ganzen auf $\varkappa \,.\, 2^\mu$ verschiedene Arten erzeugt, wo $\varkappa$ die ebendaselbst festgesetzte, nur von D und σ abhängige Bedeutung hat. Die sämmtlichen h Formen des Systemes S zerfallen nun in zwei Gruppen, nämlich in eine Gruppe von H Formen, die wir mit (a, b, c) bezeichnen wollen, für welche $\chi(m) = +1$ ist, und in

*) Auch ohne Hülfe derselben gelangt man auf einem etwas kürzern, wenn auch principiell nicht verschiedenen Wege zum Ziele, wenn man von der aus §. 91 folgenden Gleichung $\varkappa\, \Sigma\, \tau_n \psi(n) = \Sigma\, \psi(\nu)$ ausgeht, wo ψ eine willkürliche Function, und $\sigma\nu$ alle die Zahlen bedeutet, welche durch das System der Formen (a, b, c) unter den Bedingungen I., II. des §. 90 erzeugt werden. Setzt man dann $\psi(n) = n^{-s}\, \Pi(1 + \gamma_r C)$, wo γ_r den Werth des Charakters C im Geschlechte G_r bedeutet, so wird dies letztere rechts sofort isolirt, während der Grenzprocess auf der linken Seite für jeden Bestandtheil $c_r\, \chi(n)$ des Productes $\Pi(1 + \gamma_r C)$ einzeln ausgeführt werden kann.

eine zweite Gruppe von H' Formen, die wir mit (a', b', c') bezeichnen wollen, für welche $\chi(m) = -1$ ist. Offenbar werden auf diese Weise alle g_r Formen des Systems S, welche einem und demselben Geschlecht G_r angehören, auch einer und derselben dieser beiden Gruppen zugetheilt; denn für alle diese Formen hat jeder Factor von $\chi(m)$ für sich genommen und folglich auch $\chi(m)$ selbst einen und denselben Werth. Und umgekehrt leuchtet ein, dass alle Zahlen σm, denen $\chi(m) = +1$ entspricht, ausschliesslich durch Formen der ersten Gruppe, und alle Zahlen σm, denen $\chi(m) = -1$ entspricht, ausschliesslich durch Formen der zweiten Gruppe erzeugt werden.

Mithin ist

$$\varkappa \, \Sigma \, \chi(m) \, \frac{2^\mu}{m^s} = \left\{ \begin{array}{l} + \Sigma \left(\dfrac{a x^2 + 2 b x y + c y^2}{\sigma}\right)^{-s} + \cdots \\ - \Sigma \left(\dfrac{a' x^2 + 2 b' x y + c' y^2}{\sigma}\right)^{-s} - \cdots \end{array} \right\},$$

wo auf der rechten Seite die den H Formen (a, b, c) der ersten Gruppe entsprechenden Doppelsummen mit positivem Vorzeichen, und die den H' Formen (a', b', c') der zweiten Gruppe entsprechenden Doppelsummen mit negativem Vorzeichen behaftet sind.

Multiplicirt man jetzt die Gleichung mit der unendlichen Reihe

$$\Sigma \, \frac{1}{n^{2s}},$$

so erhält man links zufolge der obigen Gleichung das Resultat

$$\varkappa \, \Sigma \, \frac{\chi(n)}{n^s} \, \Sigma \left(\frac{D}{n}\right) \frac{\chi(n)}{n^s};$$

führt man ferner auf der rechten Seite die Multiplication wie in §. 90 aus, so verändert sich äusserlich ihre Gestalt nicht, sondern es fällt allein die frühere Bedingung III. fort, nach welcher die den Variabeln x, y beigelegten Werthe relative Primzahlen zu einander sein mussten. Man erhält daher

$$\varkappa \, \Sigma \, \frac{\chi(n)}{n^s} \, \Sigma \left(\frac{D}{n}\right) \frac{\chi(n)}{n^s} = \left\{ \begin{array}{l} + \Sigma \left(\dfrac{a x^2 + 2 b x y + c y^2}{\sigma}\right)^{-s} + \cdots \\ - \Sigma \left(\dfrac{a' x^2 + 2 b' x y + c' y^2}{\sigma}\right)^{-s} - \cdots \end{array} \right\}.$$

Setzen wir jetzt $s = 1 + \varrho$, und multipliciren wir mit ϱ, so nähert sich mit unendlich abnehmendem positiven ϱ jedes der h Producte

$$\varrho\,\Sigma\left(\frac{ax^2+2bxy+cy^2}{\sigma}\right)^{-(1+\varrho)}\cdots\ \varrho\,\Sigma\left(\frac{a'x^2+2b'xy+c'y^2}{\sigma}\right)^{-(1+\varrho)}\cdots$$

einem und demselben von Null verschiedenen Grenzwerth W, welcher für eine negative Determinante in §. 95, für eine positive in §. 98 bestimmt ist; mithin wird der Grenzwerth, welchem sich das Product aus ϱ und aus der rechten Seite der vorstehenden Gleichung nähert, gleich $(H - H')\,W$.

Für die beiden Fälle nun, in welchen für $\chi(n)$ entweder das Anfangsglied 1 oder das Glied $\Pi\,C'$ der Entwicklung des Productes $\Pi(1+C)$ genommen wird, ist $H = h$ und $H' = 0$; und die obige Gleichung stimmt genau mit der in §. 90 überein, welche später zur Bestimmung der Classenanzahl h führte. In den übrigen $(2\tau - 2)$ Fällen, d. h. also, wenn unter $\chi(n)$ irgend ein Glied des entwickelten Ausdrucks

$$\Pi\,(1+C) - 1 - \Pi\,C'$$

verstanden wird, nähert sich aber, wie im folgenden Paragraphen nachträglich gezeigt werden soll, jede der beiden unendlichen Reihen

$$\Sigma\,\frac{\chi(n)}{n^{1+\varrho}} \quad \text{und} \quad \Sigma\left(\frac{D}{n}\right)\frac{\chi(n)}{n^{1+\varrho}}$$

mit unendlich abnehmendem ϱ einem *endlichen* Grenzwerth, und folglich das Product

$$\varrho\,\varkappa\,\Sigma\,\frac{\chi(n)}{n^{1+\varrho}}\cdot\Sigma\left(\frac{D}{n}\right)\frac{\chi(n)}{n^{1+\varrho}}$$

dem Grenzwerth Null. Vergleicht man dies mit dem oben gefundenen Grenzwerth $(H - H')\,W$, wo W eine von Null verschiedene Grösse war, so ergiebt sich

$$H - H' = 0,$$

d. h. jedem dieser $(2\tau - 2)$ Fälle entspricht eine Eintheilung aller h Formen des Systems S in zwei Gruppen, deren jede eine gleiche Anzahl $H = H' = \frac{1}{2}h$ Formen enthält.

Zufolge der obigen Bemerkung, dass die g_r Formen des Systems S, welche einem und demselben Geschlecht G_r angehören, bei jeder einzelnen Specialisirung von $\chi(n)$ entweder alle in die erste, oder alle in die zweite Gruppe fallen, lässt sich jede solche Gleichung von der Form $H - H' = 0$, welche einem dieser $(2\tau - 2)$ Fälle entspricht, in folgender Weise aufschreiben

$$g_1 \pm g_2 \pm g_3 \pm \cdots \pm g_\tau = 0, \qquad (g)$$

wo die Anzahl g_1 jedesmal mit positivem, irgend eine andere Anzahl g_r aber mit positivem oder negativem Vorzeichen behaftet ist, je nachdem in diesem Fall die Formen des Geschlechts G_r derselben Gruppe angehören, wie die Formen des Geschlechts G_1, oder nicht, d. h. je nachdem die Werthe, welche $\chi(n)$ in dem Geschlecht G_1 und in dem Geschlecht G_r erhält, gleich oder entgegengesetzt sind. Ist $\varDelta$ der Ueberschuss der Anzahl der Fälle, in welchen das Erstere eintritt, über die Anzahl der übrigen, so wird, wenn man alle Gleichungen (g) addirt, die den $(2\tau - 2)$ verschiedenen Fällen entsprechen, der Coefficient von g_1 gleich $(2\tau - 2)$, und der von g_r gleich $\varDelta$ werden. Um nun diesen Ueberschuss $\varDelta$ zu bestimmen, bezeichnen wir mit γ_1 und γ_r die bestimmten Werthe ± 1, welche irgend einer der λ Charaktere C resp. in dem Geschlecht G_1 und G_r annimmt, und unter diesen mit γ_1' und γ_r' diejenigen Werthe, welche den Charakteren C' entsprechen; man überzeugt sich dann leicht, dass

$$\varDelta = \Pi\,(1 + \gamma_1 \gamma_r) - 1 - \Pi\,\gamma_1' \gamma_r'$$

ist; denn wenn wir das erste, aus λ Factoren von der Form $(1 + \gamma_1 \gamma_r)$ bestehende, Product rechter Hand entwickeln und die daraus entstehenden beiden Glieder 1 und $\Pi\,\gamma_1' \gamma_r'$ gegen die beiden andern Glieder fortheben, so bleiben $2^\lambda - 2 = 2\tau - 2$ Glieder zurück, deren jedes einem bestimmten Gliede des entwickelten Ausdrucks

$$\Pi\,(1 + C) - 1 - \Pi\,C',$$

d. h. einer bestimmten Specialisirung von $\chi(n)$ entspricht, und zwar wird ein solches Glied $= +1$ oder $= -1$ werden, je nachdem die beiden Werthe, welche das correspondirende $\chi(n)$ im Geschlecht G_1 und im Geschlecht G_r annimmt, gleich oder entgegengesetzt ausfallen; die algebraische Summe aller dieser Glieder ist also in der That gleich dem Ueberschuss $\varDelta$, was zu beweisen war. Da nun die beiden Geschlechter G_1 und G_r verschieden sind, so ist mindestens einer der λ Factoren $(1 + \gamma_1 \gamma_r)$ gleich Null, und da ausserdem $\Pi\,\gamma_1' = 1$, $\Pi\,\gamma_r' = 1$ und folglich auch $\Pi\,\gamma_1' \gamma_r' = 1$ ist, so erhalten wir $\varDelta = -2$. Da dieser Ueberschuss $\varDelta$ nun für alle von G_1 verschiedenen Geschlechter gleich gross ist, so erhalten wir durch Addition sämmtlicher $(2\tau - 2)$ Gleichungen (g) das Resultat

$$(2\tau - 2)\, g_1 - 2\,(g_2 + g_3 + \cdots + g_\tau) = 0,$$

und da ausserdem

$$g_1 + g_2 + g_3 + \cdots + g_\tau = h$$

ist, so folgt

$$2\tau g_1 - 2h = 0, \quad \text{also} \quad g_1 = \frac{h}{\tau} = \frac{h}{2^{\lambda-1}}.$$

Da endlich für jedes andere Geschlecht $G_2, G_3 \ldots G_\tau$ die Untersuchung ebenso geführt werden kann, wie für das Geschlecht G_1, so erhalten wir als Endresultat den Satz*):

Die Anzahl der wirklich existirenden Geschlechter ist gleich $2^{\lambda-1}$, *und alle diese Geschlechter enthalten gleich viele Formenclassen.*

§. 126.

Zur Vervollständigung des vorstehenden Beweises haben wir nun noch zu zeigen, dass für jede der $2\tau - 2$ Specialisirungen von $\chi(n)$, welche den Gliedern des obigen entwickelten Ausdrucks entsprechen, jede der beiden unendlichen Reihen

$$\Sigma \frac{\chi(n)}{n^{1+\varrho}}, \quad \Sigma \left(\frac{D}{n}\right) \frac{\chi(n)}{n^{1+\varrho}}$$

mit unendlich abnehmendem positiven ϱ sich einem endlichen Grenzwerth nähert. Dies kann mit Rücksicht auf frühere Untersuchungen (§. 101) in folgender Weise geschehen.

Jede der beiden in Rede stehenden Summen ist von der Form

$$\Sigma \frac{a_n}{n^s} = \Sigma\, \theta^{\frac{1}{2}(n-1)}\, \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{L}\right) \frac{1}{n^s},$$

*) *Gauss: D. A.* artt. 252, 261, 287. — Mit Hülfe des Satzes über die arithmetische Progression (Supplement VI.) lässt sich der obige Satz sehr kurz beweisen. Da nämlich alle Zahlen n, für welche jeder der λ Charaktere C einen vorgeschriebenen Werth ± 1 besitzt, in gewissen arithmetischen Reihen enthalten sind, deren Differenz $4D$ ist, während ihre Anfangsglieder relative Primzahlen zu $4D$ sind (vergl. §. 52), so existiren unter diesen Zahlen n auch *Primzahlen* p; genügen nun die für die Charaktere C vorgeschriebenen Werthe ± 1 der Bedingung $\Pi C' = +1$, so ist D *quadratischer Rest von* p, und folglich existirt eine (positive) ursprüngliche Form erster Art, deren erster Coefficient $= p$ ist, welche mithin den vorgeschriebenen Total-Charakter besitzt.

wo $\theta^2 = 1$, $\eta^2 = 1$, und L irgend ein ungerader Divisor von D ist; da quadratische Factoren im Nenner eines Jacobi'schen Symbols fortgelassen werden dürfen, so können wir annehmen, dass L durch keine Quadratzahl (ausser 1) theilbar ist. Ferner ist jedenfalls nicht gleichzeitig $\theta = +1$, $\eta = +1$, $L = 1$; denn sonst wäre entweder $\chi(n) = 1$, oder $\chi(n) = \Pi C'$, gegen unsere Voraussetzung.

Bezeichnen wir mit LL' das Product aus allen von einander verschiedenen in D aufgehenden ungeraden Primzahlen, so ist das System der Zahlen n identisch mit dem System aller positiven ganzen Zahlen, welche relative Primzahlen zu $8LL'$ sind; wir betrachten zunächst nur die ersten $\varphi(8LL')$ Zahlen n, d. h. diejenigen Zahlen n, welche kleiner als $8LL'$ sind, und zeigen, dass die Summe der entsprechenden Werthe von α_n gleich Null ist. Zu diesem Zwecke bezeichnen wir mit a irgend eine der vier Zahlen 1, 3, 5, 7; mit b irgend eine der $\varphi(L)$ Zahlen, welche relative Primzahlen zu L und nicht grösser als L sind; endlich mit b' irgend eine der $\varphi(L')$ Zahlen, welche relative Primzahlen zu L' und nicht grösser als L' sind. Es wird dann (nach §. 25) durch die drei Congruenzen

$$n \equiv a \pmod{8}, \quad n \equiv b \pmod{L}, \quad n \equiv b' \pmod{L'}$$

eine und nur eine Zahl n bestimmt, welche relative Primzahl zu $8LL'$ und zugleich kleiner als $8LL'$ ist; und wenn jede der drei Zahlen a, b, b' unabhängig von den anderen alle ihr zukommenden Werthe durchläuft, so werden auf diese Weise auch alle $\varphi(8LL')$ Zahlen n erzeugt, die relative Primzahlen zu $8LL'$ und kleiner als $8LL'$ sind. Da nun jedesmal

$$\theta^{\frac{1}{2}(n-1)}\,\eta^{\frac{1}{8}(n^2-1)} = \theta^{\frac{1}{2}(a-1)}\,\eta^{\frac{1}{8}(a^2-1)}, \quad \left(\frac{n}{L}\right) = \left(\frac{b}{L}\right)$$

ist, so wird die über diese Werthe von n ausgedehnte Summe

$$\Sigma\, \alpha_n = \varphi(L') \,.\, \Sigma\, \theta^{\frac{1}{2}(a-1)}\,\eta^{\frac{1}{8}(a^2-1)} \,.\, \Sigma \left(\frac{b}{L}\right);$$

nun ist aber (nach §. 52, I.)

$$\Sigma \left(\frac{b}{L}\right) = 0,$$

ausgenommen, wenn $L = 1$ ist; ausserdem findet man leicht, dass auch

$$\Sigma\, \theta^{\frac{1}{2}(a-1)}\,\eta^{\frac{1}{8}(a^2-1)} = 0$$

ist, ausgenommen, wenn $\theta = \eta = +1$ ist. Da nun, wie schon oben bemerkt ist, diese beiden Ausnahmefälle jedenfalls nicht gleichzeitig eintreten, so ist

$$\Sigma\, \alpha_n = 0,$$

wo das Summenzeichen sich auf die angegebenen Werthe von n bezieht.

Da ferner, sobald $n' \equiv n \pmod{8LL'}$, auch $\alpha_{n'} = \alpha_n$ ist, so wird immer

$$\Sigma\, \alpha_n = 0$$

sein, wenn die Summation auf beliebige $\varphi(8LL')$ auf einander folgende, also nach dem Modul $8LL'$ incongruente Werthe von n ausgedehnt wird. Und hieraus folgt unmittelbar, dass die Summe aller Werthe von α_n, die beliebig vielen auf einander folgenden Werthen von n entsprechen (von $n = 1$ an gerechnet) stets unterhalb einer endlichen angebbaren Grenze bleibt. Nach einer frühern Untersuchung (§. 101) ist daher die Reihe

$$\Sigma\, \frac{\alpha_n}{n^s},$$

wenn ihre Glieder nach der Grösse der Nenner geordnet werden, eine für jeden positiven Werth von s endliche und stetige Function von s; also nähert sich auch jede der beiden obigen Reihen mit unendlich abnehmendem positiven ϱ einem endlichen Grenzwerth, was zu beweisen war.

V. Theorie der Potenzreste für zusammengesetzte Moduli.

§. 127.

Es ist in §. 28 gezeigt, dass wenn die Zahl a relative Primzahl gegen den Modul k ist, stets positive ganze Exponenten n von der Beschaffenheit existiren, dass $a^n \equiv 1 \pmod{k}$ ist; diese Exponenten n sind die sämmtlichen Vielfachen des kleinsten unter ihnen; bezeichnet man diesen mit δ, so sagt man, die Zahl a *gehöre* zum Exponenten δ; und die δ Zahlen

$$1,\ a,\ a^2 \ldots a^{\delta-1} \qquad (A)$$

sind sämmtlich incongruent. Mit Hülfe des verallgemeinerten Fermat'schen Satzes ist dort ebenfalls gezeigt, dass δ immer ein Divisor von $\varphi(k)$ ist; dies Resultat lässt sich aber auch ohne Hülfe des Fermat'schen Satzes ableiten durch eine eigenthümliche Methode, welche sehr häufig zum Nachweise der Theilbarkeit einer Zahl durch eine andere gebraucht werden kann. In unserm Falle gestaltet dieselbe sich folgendermaassen.

Ist a' irgend eine relative Primzahl zu k, so sind (nach §. 18) die δ Zahlen

$$a',\ a'a,\ a'a^2 \ldots a'a^{\delta-1} \qquad (A')$$

sämmtlich incongruent; dasselbe gilt von den δ Zahlen

$$a'',\ a''a,\ a''a^2 \ldots a''a^{\delta-1} \qquad (A'')$$

sobald a'' ebenfalls relative Primzahl zu k ist. Jeder solche Complex, wie A' oder A'', enthält δ unter einander incongruente Zahlen, die sämmtlich relative Primzahlen gegen k sind und also als

Repräsentanten von δ Zahl-Classen in Bezug auf den Modul k angesehen werden können. Gesetzt nun, es findet sich eine und dieselbe Zahlclasse in jedem der beiden Complexe A' und A'' vertreten, so giebt es zwei Exponenten μ', μ'' von der Beschaffenheit, dass

$$a' . a^{\mu'} \equiv a'' . a^{\mu''} \pmod{k}$$

ist; nehmen wir an, was der Symmetrie wegen erlaubt ist, dass $\mu'' \geqq \mu'$, so erhält man durch Division mit $a^{\mu'}$ die Congruenz

$$a' \equiv a'' . a^{\mu''-\mu'} \pmod{k};$$

und hieraus folgt sogleich, dass *jede* in A' enthaltene Zahl $a' . a^m$ auch einer Zahl von der Form $a'' . a^n$, d. h. einer in A'' enthaltenen Zahl congruent ist. Wir können hieraus schliessen, dass entweder zwei solche Complexe A', A'' dieselben δ Zahlclassen enthalten, oder dass keine einzige Classe in beiden gleichzeitig vertreten ist.

Bildet man nun der Reihe nach alle solche aus δ Zahlclassen bestehenden Complexe von der Form A', A'' ..., und zwar nur solche, welche von einander verschieden sind, so muss endlich jede der $\varphi(k)$ Zahlclassen, welche relative Primzahlen zu k enthalten, in einem dieser Complexe, und auch nur in einem, vertreten sein; ist daher ε die Anzahl dieser von einander verschiedenen Complexe, so muss $\varphi(k) = \varepsilon\delta$, also $\varphi(k)$ theilbar durch δ sein, was zu beweisen war.

Hieraus ergiebt sich nun der Fermat'sche Satz als Folgerung; denn erhebt man die Congruenz

$$a^{\delta} \equiv 1 \pmod{k}$$

zur εten Potenz, so erhält man

$$a^{\varphi(k)} \equiv 1 \pmod{k}.$$

§. 128.

Für den Fall, dass der Modul k eine Primzahl p ist, wurde ferner in §. 29 bewiesen, dass zu jedem Divisor δ von $\varphi(p) = p - 1$ genau $\varphi(\delta)$ Zahlen gehören, die nach dem Modul p incongruent sind; und in §. 30 sind die Eigenschaften der sogenannten primi-

tiven Wurzeln von p betrachtet, d. h. derjenigen $\varphi(p-1)$ incongruenten Zahlen g, welche zum Exponenten $p-1$ selbst gehören. Wir wollen nun untersuchen, ob ähnliche Gesetze auch für zusammengesetzte Moduln gelten.

Zunächst beschränken wir uns auf den Fall, in welchem der Modul k eine *Potenz von einer ungeraden Primzahl* p ist, und wir werden der Analogie nach unter einer *primitiven Wurzel* von k jede Zahl g verstehen, welche zum Exponenten $\varphi(k)$ gehört. Dem Beweise der wirklichen Existenz solcher primitiven Wurzeln schicken wir folgenden Hülfssatz voraus:

Ist h irgend eine ganze Zahl und $\pi \geqq 1$ eine positive ganze Zahl, so ist stets

$$(1+hp^\pi)^p \equiv 1 + hp^{\pi+1} \pmod{p^{\pi+2}}.$$

Man überzeugt sich hiervon leicht durch die Entwicklung der linken Seite nach dem binomischen Satze; man findet nämlich zunächst, indem man sich auf die drei ersten Glieder beschränkt,

$$(1+hp^\pi)^p \equiv 1 + hp^{\pi+1} + \tfrac{1}{2}(p-1)h^2p^{2\pi+1} \pmod{p^{3\pi}},$$

und hieraus ergiebt sich die obige Congruenz, wenn man bedenkt, dass p ungerade, also $\frac{1}{2}(p-1)$ eine ganze Zahl, und ferner, dass sowohl $p^{2\pi+1}$ als auch $p^{3\pi}$ durch $p^{\pi+2}$ theilbar ist.

Nach dieser Vorbemerkung gehen wir an unsere Untersuchung und nehmen zunächst einmal an, es existire für den Modul $p^{\pi+1}$, wo $\pi \geqq 1$ ist, wirklich eine primitive Wurzel g; dann liegt es nahe zu fragen: zu welchem Exponenten gehört eine solche Zahl g in Bezug auf den Modul p^π? Es sei δ dieser Exponent, also

$$g^\delta = 1 + hp^\pi,$$

so erhält man mit Hülfe des soeben bewiesenen Satzes

$$g^{\delta p} \equiv 1 \pmod{p^{\pi+1}};$$

da nun g primitive Wurzel von $p^{\pi+1}$ ist, so muss δp durch $\varphi(p^{\pi+1}) = (p-1)p^\pi$, und folglich δ durch $(p-1)p^{\pi-1}$ theilbar sein; andererseits muss aber, da g zum Exponenten δ in Bezug auf den Modul p^π gehört, nothwendig $\varphi(p^\pi) = (p-1)p^{\pi-1}$ durch δ theilbar sein; mithin ist $\delta = \varphi(p^\pi)$, d. h. g ist auch primitive Wurzel von p^π. Zugleich leuchtet ein, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^\pi$$

vorkommende Zahl h nicht durch p theilbar sein kann; denn sonst wäre

$$g^{(p-1)p^{\pi-1}} \equiv 1 \text{ (mod. } p^{\pi+1}),$$

also g keine primitive Wurzel von $p^{\pi+1}$.

Setzt man diese Schlüsse weiter fort, so erhält man zunächst das Resultat:

Jede primitive Wurzel g von einer höhern Potenz einer ungeraden Primzahl p ist nothwendig eine primitive Wurzel der Zahl p selbst, und zwar von der Beschaffenheit, dass $g^{p-1}-1$ nicht durch p^2 theilbar ist.

Wir wollen nun umgekehrt annehmen, es sei g eine primitive Wurzel von p^π, und zwar von der Beschaffenheit, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^\pi$$

vorkommende Zahl h nicht durch p theilbar ist; und wir fragen jetzt: zu welchem Exponenten gehört diese Zahl g in Bezug auf den Modul $p^{\pi+1}$? Ist δ dieser Exponent, also

$$g^\delta \equiv 1 \text{ (mod. } p^{\pi+1}),$$

so ist auch

$$g^\delta \equiv 1 \text{ (mod. } p^\pi),$$

und folglich δ theilbar durch $\varphi(p^\pi)$; da aber andererseits δ ein Divisor von $\varphi(p^{\pi+1}) = p\varphi(p^\pi)$ sein muss, so ist δ entweder $= \varphi(p^\pi)$, oder $= \varphi(p^{\pi+1})$; das Erstere ist aber nicht der Fall, weil unserer Voraussetzung zufolge die Zahl h nicht durch p theilbar ist; also ist $\delta = \varphi(p^{\pi+1})$, d. h. die Zahl g ist primitive Wurzel von $p^{\pi+1}$. Zugleich leuchtet aus der Congruenz

$$g^{(p-1)p^\pi} = (1 + hp^\pi)^p \equiv 1 + hp^{\pi+1} \text{ (mod. } p^{\pi+2})$$

ein, dass die in der Gleichung

$$g^{(p-1)p^\pi} = 1 + h'p^{\pi+1}$$

vorkommende Zahl h' nicht durch p theilbar ist.

Durch Fortsetzung dieser Schlussweise erhalten wir das zweite Resultat:

Jede primitive Wurzel g einer ungeraden Primzahl p, für welche die Differenz $g^{p-1}-1$ nicht durch p^2 theilbar ist, ist auch eine primitive Wurzel aller höheren Potenzen von p.

Um also die Existenz von primitiven Wurzeln g für höhere Potenzen von p nachzuweisen, und um alle diese Zahlen g zu finden, haben wir nur noch zu zeigen, dass in der That primitive Wurzeln g von p existiren, für welche $g^{p-1}-1$, oder, was dasselbe sagt, für welche g^p-g nicht durch p^2 theilbar ist. Dies geschieht leicht auf folgende Weise. Ist f irgend eine primitive Wurzel von p, so sind alle in der Form

$$g = f + px$$

enthaltenen Zahlen g ebenfalls primitive Wurzeln von p; dann ist nach dem binomischen Satze

$$g^p \equiv f^p \pmod{p^2};$$

setzen wir daher

$$f^p \equiv f + f'p \pmod{p^2},$$

so wird

$$g^p - g \equiv p(f' - x) \pmod{p^2},$$

und folglich ist $g = f + px$ jedesmal eine primitive Wurzel aller Potenzen von p, ausgenommen, wenn $x \equiv f' \pmod{p}$, also

$$g \equiv f^p \pmod{p^2}$$

ist. Da nun $\varphi(p-1)$ nach dem Modul p incongruente Zahlen f existiren, und aus jeder Zahl f genau $(p-1)$ in Bezug auf den Modul p^2 incongruente Zahlen $g = f + px$ von der Beschaffenheit abgeleitet werden können, dass $g^{p-1}-1$ nicht durch p^2 theilbar wird, so erhalten wir das Resultat:

Die sämmtlichen primitiven Wurzeln von höheren Potenzen einer ungeraden Primzahl p sind die sämmtlichen Individuen von $(p-1)\varphi(p-1)$ verschiedenen Zahlclassen in Bezug auf den Modul p^2.

Beispiel: Sämmtliche primitive Wurzeln der Primzahl $p = 7$ sind in den beiden Reihen $7x+3$, $7x+5$ enthalten; da nun

$$3^7 \equiv 31,\quad 5^7 \equiv 19 \pmod{49}$$

ist, so sind alle in den arithmetischen Reihen $7x+3$, $7x+5$ enthaltenen Zahlen, mit Ausnahme derer, welche $\equiv 31$ oder $\equiv 19 \pmod{49}$ sind, auch primitive Wurzeln von allen höheren Potenzen von 7.

§. 129.

Nachdem im Vorhergehenden die Existenz von primitiven Wurzeln g für jeden Modul p^π nachgewiesen ist, der eine Potenz einer ungeraden Primzahl p ist, kann man leicht die übrigen elementaren Fragen über die Potenzreste beantworten. Setzt man zur Abkürzung

$$\varphi(p^\pi) = c,$$

so sind die Potenzen

$$g^0, g^1, g^2 \ldots g^{c-1} \pmod{p^\pi}$$

sämmtlich incongruent, und bilden daher ein vollständiges System incongruenter Zahlen, mit Ausschluss der durch p theilbaren Zahlen. Ist daher n irgend eine durch p nicht theilbare Zahl, so existiren stets unendlich viele Exponenten γ, die aber nach dem Modul c sämmtlich einander congruent sind, von der Beschaffenheit, dass

$$n \equiv g^\gamma \pmod{p^\pi};$$

man nennt dann γ den *Index der Zahl* n *für die Basis* g, und drückt dies in Zeichen so aus

$$\text{Ind. } n \equiv \gamma \pmod{c};$$

durchläuft γ ein vollständiges Restsystem in Bezug auf den Modul c, so durchläuft n ein vollständiges System von Zahlen, die relative Primzahlen zu p^π und unter einander nach dem Modul p^π incongruent sind. Für die Rechnung mit diesen Indices gelten dieselben Gesetze, wie die (in §. 30 angegebenen) für den Fall $\pi = 1$. Wir heben hier besonders hervor, dass

$$\text{Ind. }(1) \equiv 0, \quad \text{Ind. }(-1) \equiv \tfrac{1}{2}c \pmod{c},$$

und ferner, dass n quadratischer Rest oder Nichtrest von p^π ist, je nachdem Ind. n gerade oder ungerade ist.

Aus dem Index einer Zahl n lässt sich leicht der Exponent t bestimmen, zu welchem n in Bezug auf den Modul p^π gehört; aus

$$n \equiv g^{\text{Ind.} n} \pmod{p^\pi}$$

folgt nämlich

$$n^t \equiv g^{t\,\mathrm{Ind}.\,n} \pmod{p^\pi};$$

soll also $n^t \equiv 1$ sein, so muss t Ind. n durch c theilbar, und folglich t ein Multiplum von $c:\delta$ sein, wo δ den grössten gemeinschaftlichen Divisor von c und Ind. n bedeutet; die kleinste aller dieser Zahlen t, d. h. der Exponent, zu welchem n gehört, ist daher $= c:\delta$.

Hieraus folgt, dass n stets und nur dann eine primitive Wurzel von p^π ist, wenn Ind. n relative Primzahl zu c ist; die Anzahl aller nach dem Modul p^π incongruenten primitiven Wurzeln von p^π ist daher gleich der Anzahl derjenigen der Zahlen

$$0,\ 1,\ 2 \ldots c-1,$$

welche relative Primzahlen zu c sind, also gleich $\varphi(c) = \varphi\varphi(p^\pi)$. Dasselbe Resultat ist aber auch eine unmittelbare Folge aus dem Schlusssatze des vorigen Paragraphen.

§. 130.

Die Primzahl 2 verhält sich anders als die ungeraden Primzahlen, welche bisher ausschliesslich betrachtet wurden.

Für den Modul 2 kann jede ungerade Zahl als primitive Wurzel angesehen werden.

Für den Modul $2^2 = 4$ ist $3 \equiv -1$ eine primitive Wurzel; zu jeder ungeraden Zahl n giebt es einen entsprechenden Exponenten α von der Beschaffenheit, dass

$$n \equiv (-1)^\alpha \pmod{4}$$

ist; und zwar ist $\alpha \equiv 0 \pmod{2}$ oder $\equiv 1 \pmod{2}$, je nachdem $n \equiv 1$ oder $\equiv 3 \pmod{4}$ ist.

Bis hierher findet also noch völlige Analogie mit den ungeraden Primzahlen Statt; sobald aber ein Modul 2^λ betrachtet wird, in welchem der Exponent $\lambda \geqq 3$ ist, hört dieselbe auf. Es lässt sich nämlich zeigen, dass, wenn n irgend eine ungerade Zahl bedeutet, immer schon

$$n^{\frac{1}{2}\varphi(2^\lambda)} = n^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}$$

ist. In der That ist dieser Satz richtig für $\lambda = 3$; denn das Quadrat jeder ungeraden Zahl n ist $\equiv 1 \pmod{8}$. Nehmen wir

ferner an, der Satz sei für einen beliebigen Exponenten $\lambda \geqq 3$ schon bewiesen, es sei also

$$n^{2^{\lambda-2}} = 1 + h\,2^{\lambda},$$

so folgt hieraus durch Quadriren

$$n^{2^{\lambda-1}} = 1 + h\,2^{\lambda+1} + h^2 2^{2\lambda} \equiv 1 \pmod{2^{\lambda+1}},$$

d. h. der Satz gilt auch für den nächstfolgenden Exponenten $\lambda + 1$. Er gilt mithin allgemein, da er für $\lambda = 3$ gilt.

Es fragt sich nun, ob es in diesen Fällen wenigstens Zahlen giebt, die zu dem Exponenten $\frac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2}$ gehören; man überzeugt sich leicht, dass die Zahl 5 diese Eigenschaft für jeden Modul $2^{\lambda} \geqq 8$ besitzt. Es ist nämlich

$$5 \equiv 1 + 4 \pmod{8}$$
$$5^2 \equiv 1 + 8 \pmod{16}$$
$$5^4 \equiv 1 + 16 \pmod{32}$$
$$5^8 \equiv 1 + 32 \pmod{64}$$

allgemein

$$5^{2^{\lambda-3}} \equiv 1 + 2^{\lambda-1} \pmod{2^{\lambda}},$$

also

$$5^{2^{\lambda-3}} \text{ niemals} \equiv 1 \pmod{2^{\lambda}},$$

woraus unmittelbar folgt, dass der Exponent, zu welchem die Zahl 5 nach dem Modul 2^{λ} gehört, kein Divisor von $2^{\lambda-3}$ sein kann, und also, da er doch Divisor von $2^{\lambda-2}$ sein muss, nothwendig $= 2^{\lambda-2}$ ist.

Hieraus ergiebt sich nun, wenn man zur Abkürzung

$$\tfrac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2} = b$$

setzt, dass die b Zahlen

$$5^0,\ 5^1,\ 5^2 \ldots 5^{b-1}$$

sämmtlich nach dem Modul 2^{λ} incongruent sind; dasselbe gilt von den Zahlen

$$-5^0,\ -5^1,\ -5^2 \ldots -5^{b-1}$$

da ferner die erstern sämmtlich $\equiv 1 \pmod{4}$, die letztern sämmtlich $\equiv 3 \pmod{4}$ sind, so bilden sie zusammengenommen ein System von $\varphi(2^{\lambda})$ nach dem Modul 2^{λ} incongruenten ungeraden Zahlen. Ist daher n irgend eine ungerade Zahl, so kann man stets

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$

setzen, wo α nach dem Modul 2, und β nach dem Modul b vollständig bestimmt ist. Durchläuft α ein vollständiges Restsystem in Bezug auf den Modul 2, und β unabhängig von α ein vollständiges Restsystem in Bezug auf den Modul b, so durchläuft n ein vollständiges System von Zahlen, die in Bezug auf den Modul 2^{λ} incongruent und relative Primzahlen zu 2^{λ}, d. h. ungerade sind. Diese beiden Zahlen α und β kann man die *Indices* der Zahl n nennen; sie befolgen ganz ähnliche Gesetze, wie die Indices für die früher betrachteten Moduli. Wir heben noch besonders hervor, dass $n \equiv \pm 1$ oder $\equiv \pm 3 \pmod{8}$ ist, je nachdem β gerade oder ungerade.

Es verdient bemerkt zu werden, dass die vorstehende Form, in welche jede ungerade Zahl n gebracht werden kann, auch noch für den Fall $\lambda = 2$ gilt; die Anzahl b der Werthe von β reducirt sich nämlich auf 1, und da $5 \equiv 1 \pmod{4}$, so geht die obige Form in die frühere $n \equiv (-1)^{\alpha} \pmod{4}$ über. Für eine spätere Untersuchung ist es sogar zweckmässig, dieselbe Form der Darstellung aller relativen Primzahlen zu einem Modul von der Form 2^{λ} auf die Fälle $\lambda = 0$ und $\lambda = 1$ auszudehnen; da in denselben nur eine einzige Zahlclasse darzustellen ist, so wird man α und β auch nur einen einzigen Werth beizulegen haben; setzen wir daher $a = b = 1$, wenn $\lambda = 0$ oder $\lambda = 1$ ist, in allen anderen Fällen $(\lambda \geqq 2)$ aber $a = 2$, $b = \frac{1}{2}\varphi(2^{\lambda})$, so können wir sagen, dass der Ausdruck

$$n \equiv (-1)^{\alpha} 5^{\beta} \pmod{2^{\lambda}}$$

alle incongruenten relativen Primzahlen zum Modul durchläuft, wenn α und β resp. vollständige Restsysteme in Bezug auf a und b durchlaufen.

§. 131.

Es sei nun der Modul eine beliebige zusammengesetzte Zahl

$$k = 2^{\lambda} p^{\pi} p'^{\pi'} \ldots,$$

wo p, p' von einander verschiedene ungerade Primzahlen, und λ, π, π' . . . ganze positive Exponenten bedeuten, deren erster, λ,

auch $= 0$ sein kann. Ist n irgend eine relative Primzahl zu k, so kann man stets

$$n \equiv (-1)^\alpha 5^\beta \pmod{2^\lambda}$$
$$n \equiv g^\gamma \pmod{p^\pi}$$
$$n \equiv g'^{\gamma'} \pmod{p'^{\pi'}}$$
$$\dots\dots\dots\dots\dots$$

setzen, wo g, g' ... primitive Wurzeln resp. von p^2, p'^2 ... bedeuten. Geben wir den Zahlen a, b die im vorigen Paragraphen festgesetzte Bedeutung und setzen wir zur Abkürzung

$$\varphi(p^\pi) = c, \quad \varphi(p'^{\pi'}) = c' \dots,$$

so sind die Exponenten oder Indices

$$\alpha, \ \beta, \ \gamma, \ \gamma' \dots$$

vollständig bestimmt in Bezug auf die entsprechenden Moduli

$$a, \ b, \ c, \ c' \dots,$$

und umgekehrt entspricht jedem solchen Systeme von Indices (nach §. 25) eine bestimmte Classe von Zahlen n nach dem Modul k, die relative Primzahlen zu k sind. Durchlaufen die Indices α, β, γ, γ' ... unabhängig von einander ihre a, b, c, c' ... Werthe, so durchläuft n sämmtliche

$$abcc' \dots = \varphi(k)$$

Zahlclassen in Bezug auf den Modul k, welche relative Primzahlen zu k enthalten.

Sind die Indices α, β, γ, γ' ... einer Zahl n bekannt, so ist es leicht, den Exponenten δ zu bestimmen, zu welchem die Zahl n gehört; denn offenbar ist δ das kleinste gemeinschaftliche Multiplum aller derjenigen Exponenten, zu welchen die Zahl n in Bezug auf die einzelnen Moduli 2^λ, p^π, $p'^{\pi'}$ ... gehört. Dieser Exponent δ ist daher immer ein Divisor von dem kleinsten gemeinschaftlichen Vielfachen μ der Zahlen a, b, c, c' ... Es können daher primitive Wurzeln von k, d. h. Zahlen, die zum Exponenten $\varphi(k)$ gehören, nur dann existiren, wenn $\mu = \varphi(k)$ ist; man überzeugt sich leicht, dass dies nur dann der Fall ist, wenn der Modul $k = 1$, ~~oder $= 2$,~~ oder $= 4$, oder eine Potenz einer ungeraden Primzahl, oder das Doppelte einer solchen Potenz ist; und umgekehrt leuchtet ein, dass in diesen Fällen immer primitive Wurzeln existiren.

Da ferner die Möglichkeit einer binomischen Congruenz von der Form

$$x^m \equiv n \pmod{k}$$

und die Anzahl ihrer Wurzeln nur von der Möglichkeit derselben Congruenz in Bezug auf die einzelnen Moduli 2^λ, p^π, $p'^{\pi'}$ ... abhängt (nach §. 37), so überzeugt man sich leicht, dass zur Beurtheilung dieser Frage und zur Auffindung der Wurzeln der Congruenz die Kenntniss der Indices der Zahl n vollständig ausreicht. Die wirkliche Ausführung dieser Untersuchung unterdrücken wir hier, weil sie sich ganz ebenso gestaltet wie in §. 31. Der Fall $m = 2$ würde auf diese Weise behandelt auf das in §. 37 gewonnene Resultat zurückführen. Ebenso leicht ist es, den verallgemeinerten Wilson'schen Satz (§. 38) von Neuem zu beweisen.

VI. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.

§. 132.

Der allgemeine Beweis dieses Satzes*) stützt sich auf die Betrachtung einer Classe von unendlichen Reihen von der Form

$$L = \Sigma\, \psi(n),$$

wo der Buchstabe n alle ganzen positiven Zahlen durchlaufen muss, und die reelle oder complexe Function $\psi(n)$ der Bedingung

$$\psi(n)\,\psi(n') = \psi(nn')$$

genügt. Hieraus folgt für $n = n' = 1$, dass $\psi(1) = 1$ oder $= 0$ ist; da aber im letztern Fall $\psi(n) = \psi(1)\,\psi(n)$ für alle Werthe von n verschwinden würde, so nehmen wir immer an, dass $\psi(1) = 1$ ist. Wir nehmen ferner an, die Function $\psi(n)$ sei so beschaffen, dass die Summe der analytischen Moduln aller Werthe $\psi(n)$ *endlich* ist, woraus folgt, dass die Reihe L einen von der Anordnung ihrer Glieder unabhängingen endlichen Werth besitzt. Man überzeugt sich dann leicht von der Richtigkeit der folgenden Gleichung

$$\Pi \frac{1}{1 - \psi(q)} = \Sigma\, \psi(n), \tag{I}$$

*) *Dirichlet:* Abhandlungen der Berliner Akademie aus dem Jahre 1837.

wo das Productzeichen sich auf alle, in beliebiger Ordnung auf einander folgenden, Primzahlen q bezieht*).

Zunächst leuchtet ein, da die Reihe L die Glieder

$$\psi(1) = 1, \quad \psi(q) = z, \quad \psi(q^2) = z^2 \dots$$

enthält, und die Summe derselben für sich einen endlichen Werth hat, dass der Modulus von $\psi(q) < 1$, und folglich

$$\frac{1}{1-\psi(q)} = 1 + \psi(q) + \psi(q^2) + \cdots$$

ist. Sind ferner $q_1, q_2, q_3 \dots$ die sämmtlichen Primzahlen q, wie sie in dem Producte linker Hand aufeinander folgen, so wird das Product Q der ersten m Factoren

$$\frac{1}{1-\psi(q_1)}, \ \frac{1}{1-\psi(q_2)} \cdots \frac{1}{1-\psi(q_m)},$$

wenn man jeden derselben nach der vorstehenden Gleichung in eine unendliche Reihe entwickelt und die Multiplication ausführt, gleich $\Sigma\psi(l)$, wo die Summation über alle die ganzen positiven Zahlen l auszudehnen ist, in welchen keine andern als die Primzahlen $q_1, q_2 \dots q_m$ aufgehen. Ist daher h irgend eine positive ganze Zahl, und nimmt man m so gross, dass unter den Primzahlen $q_1, q_2 \dots q_m$ sich alle diejenigen finden, welche $< h$ sind, so enthält $\Sigma\psi(l)$ alle Glieder der Reihe $\Sigma\psi(n)$, in welchen $n < h$ ist, und ausserdem noch unendlich viele andere, in denen $n > h$ ist. Mithin unterscheidet sich das Product Q von der Summe $\Sigma\psi(n)$ um eine Summe von der Form $\Sigma\psi(n')$, in welche aber nur noch Zahlen n' eingehen, welche $\geqq h$ sind. Da nun die Summe der Moduln aller Glieder $\psi(n)$ endlich ist, so kann man h, und also auch m so gross wählen, dass die Summe der Moduln aller Glieder $\psi(n')$, und folglich auch der Modul der Differenz $Q - \Sigma\psi(n)$ kleiner wird als jede vorher gegebene Grösse; d. h. mit unbegrenzt wachsendem m nähert sich Q dem Grenzwerth $\Sigma\psi(n)$, was zu beweisen war.

Ausser diesen Reihen von der Form $L = \Sigma\psi(n)$ haben wir noch diejenigen Reihen zu betrachten, welche durch die Entwick-

*) Unter dieser Classe von Reihen sind auch diejenigen enthalten, welche im fünften Abschnitt betrachtet sind. Vergl. §§. 124, 135. Der Werth einer solchen Function ψ ist offenbar für alle Zahlen vollständig bestimmt, sobald er für alle Primzahlen willkürlich angenommen ist. Die ältesten Untersuchungen über solche Reihen und Producte finden sich bei *Euler: Introductio in analysin infinitorum.* Cap. XV.

lung ihrer natürlichen Logarithmen entstehen. Wenn der Modulus von z ein echter Bruch ist, so ist bekanntlich

$$z + \frac{1}{2}z^2 + \frac{1}{3}z^3 + \frac{1}{4}z^4 + \cdots = \log \frac{1}{1-z},$$

und zwar ist der imaginäre Bestandtheil des Logarithmen rechter Hand stets zwischen den Grenzen $-\frac{1}{2}\pi i$ und $+\frac{1}{2}\pi i$ zu nehmen. Setzt man hierin $z = \psi(q)$ und für q alle Primzahlen, so erhält man zufolge der Gleichheit (I)

$$\Sigma\, \psi(q) + \tfrac{1}{2}\Sigma\, \psi(q^2) + \tfrac{1}{3}\Sigma\, \psi(q^3) + \cdots = \log L, \qquad \text{(II)}$$

und offenbar hat die aus unendlich vielen unendlichen Reihen bestehende linke Seite einen von der Anordnung der Summationen unabhängigen endlichen Werth, weil selbst die Summe der Moduln aller ihrer Glieder einen endlichen Werth besitzt. Der imaginäre Theil des Logarithmen rechter Hand ist die Summe aller imaginären Theile der Logarithmen der einzelnen Factoren, aus denen das obige unendliche Product besteht.

Wir fügen zu diesem Resultat noch einige Bemerkungen hinzu. Ist zunächst $\psi(n)$ eine reelle Function, so sind alle Factoren des unendlichen Productes positiv, also ist $\log L$ reell, und da die Reihe $\log L$ einen endlichen Werth hat, so ist L ein positiver von Null verschiedener Werth. Ist aber $\psi(n)$ imaginär, und $\psi'(n)$ der jedesmal mit $\psi(n)$ conjugirte complexe Werth, so ist auch $\psi'(n)\,\psi'(n') = \psi'(nn')$, und die über alle ganzen positiven Zahlen n ausgedehnte Summe $L' = \Sigma\,\psi'(n)$ ist die mit $L = \Sigma\,\psi(n)$ conjugirte Zahl. Zugleich wird

$$\Sigma\, \psi'(q) + \tfrac{1}{2}\,\Sigma\, \psi'(q^2) + \tfrac{1}{3}\,\Sigma\, \psi'(q^3) + \cdots = \log L',$$

und zwar ist $\log L'$ conjugirt mit $\log L$, so dass die Summe $\log L + \log L' = \log(LL')$ reell wird.

Ist endlich der Werth der Function ψ für alle in einer bestimmten Zahl k aufgehenden Primzahlen $= 0$, so ist $\psi(n)$ jedesmal $= 0$, wenn n keine relative Primzahl zu k ist, und die Gleichungen (I) und (II) bleiben richtig, wenn man n alle relativen Primzahlen zu k, und q alle in k nicht aufgehenden Primzahlen durchlaufen lässt.

§. 133.

Es sei nun (wie in §. 131) k eine beliebige positive ganze Zahl, und zwar

$$k = 2^\lambda p^\pi p'^{\pi'} \ldots,$$

wo $p, p' \ldots$ von einander verschiedene ungerade Primzahlen bedeuten; wir geben ferner den Buchstaben

$$a, \; b, \; c, \; c' \ldots$$

ihre frühere Bedeutung (§. 131) und bezeichnen entsprechend mit

$$\theta, \; \eta, \; \omega, \; \omega' \ldots$$

irgend welche Wurzeln der Gleichungen

$$\theta^a = 1, \; \eta^b = 1, \; \omega^c = 1, \; \omega'^{c'} = 1 \ldots$$

Ist nun n irgend eine positive ganze Zahl und zugleich relative Primzahl zu k, und sind ihre Indices

$$\alpha \,(\text{mod. } a), \; \beta \,(\text{mod. } b), \; \gamma \,(\text{mod. } c), \; \gamma' \,(\text{mod. } c') \ldots,$$

so genügt, wie man leicht sieht, der Ausdruck

$$\psi(n) = \frac{\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots}{n^s}$$

der Bedingung $\psi(n)\,\psi(n') = \psi(n n')$ *); wenn ferner der Exponent $s > 1$ ist, was wir im Folgenden annehmen wollen, so ist die Summe der Moduln n^{-s} aller Glieder $\psi(n)$ endlich (§. 117), und folglich gelten die Gleichungen (I) und (II) des vorigen Paragraphen

$$\Pi \frac{1}{1 - \psi(q)} = \Sigma \, \psi(n) = L$$

$$\Sigma \, \psi(q) + \tfrac{1}{2} \Sigma \, \psi(q^2) + \tfrac{1}{3} \Sigma \, \psi(q^3) + \cdots = \log L$$

in welchen q alle in k nicht aufgehenden Primzahlen, n alle relativen Primzahlen zu k durchlaufen muss; beide Reihen haben, so lange $s > 1$ ist, bestimmte von der Anordnung ihrer Glieder un-

*) Der Zähler $\chi(n) = \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots$ besitzt die charakteristischen Eigenschaften $\chi(n)\,\chi(n') = \chi(n n')$ und, wenn $n' \equiv n''$ (mod. k) ist, $\chi(n') = \chi(n'')$. Umgekehrt, wenn eine Function $\chi(n)$ die erste Eigenschaft hat, und wenn sie ausserdem nur eine *endliche* Anzahl m (von Null verschiedener) Werthe $\omega_1, \omega_2 \ldots \omega_m$ besitzt, so sind diese letzteren nothwendig die sämmtlichen Wurzeln der Gleichung $\omega^m = 1$.

abhängige Summen. Wir können hinzufügen, dass beide Reihen auch *stetige* Functionen von s sind, so lange $s > 1$ ist; wir beweisen diese Behauptung für alle Werthe von s, welche grösser als ein beliebiger unechter Bruch σ sind, weil hieraus offenbar die Stetigkeit dieser Reihen für alle Werthe von $s > 1$ (excl. 1) folgt.

Jede der beiden Reihen L und $\log L$ ist von der Form

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \frac{\alpha_3}{3^s} + \cdots,$$

wo die Moduln der Coefficienten $\alpha_1, \alpha_2, \alpha_3 \ldots$ sämmtlich eine endliche Grösse $A (= 1)$ nicht übertreffen. Um die Stetigkeit einer Function von s innerhalb eines gewissen Intervalls $(s \geqq \sigma)$ zu beweisen, genügt es darzuthun, dass, wie klein auch eine positive gegebene Grösse δ sein mag, die Function jedesmal in einen ersten und zwar stetigen, und in einen zweiten Bestandtheil zerlegt werden kann, dessen Modulus innerhalb des ganzen Intervalls $(s \geqq \sigma)$ $< \delta$ ist; denn hieraus folgt, dass der Modulus einer plötzlichen Werthänderung der ganzen Function, die doch nur von dem zweiten Bestandtheil herrühren kann, kleiner als 2δ, und folglich, da die gegebene Grösse δ beliebig klein sein darf, nothwendig $= 0$ sein muss (vergl. §§. 101, 143). In unserm Falle ergiebt sich die Möglichkeit einer solchen Zerlegung auf folgende Weise; ist n eine beliebige ganze Zahl, so ist die Summe der ersten n Glieder

$$\frac{\alpha_1}{1^s} + \frac{\alpha_2}{2^s} + \cdots + \frac{\alpha_n}{n^s}$$

eine stetige Function; der Modulus der Summe aller folgenden Glieder ist kleiner als

$$A\left(\frac{1}{(n+1)^s} + \frac{1}{(n+2)^s} + \cdots\right)$$

und folglich für *alle* Werthe $s \geqq \sigma$ auch kleiner als

$$A\left(\frac{1}{(n+1)^\sigma} + \frac{1}{(n+2)^\sigma} + \cdots\right);$$

da nun σ ein unechter Bruch ist, und folglich (nach §. 117) die Reihe

$$\frac{1}{1^\sigma} + \frac{1}{2^\sigma} + \frac{1}{3^\sigma} + \cdots$$

convergirt, so kann für jede gegebene Grösse δ entsprechend n so gross gewählt werden, dass

$$A\left(\frac{1}{(n+1)^\sigma}+\frac{1}{(n+2)^\sigma}+\cdots\right)<\delta$$

wird; hiermit ist für jede gegebene Grösse δ die Möglichkeit einer Zerlegung unserer Reihe in zwei Bestandtheile von der obigen Art, und also auch die Stetigkeit der Reihen L und $\log L$ für jeden Werth $s > 1$ nachgewiesen.

Der Beweis des Satzes über die arithmetische Progression gründet sich nun auf die Untersuchung des Verhaltens der Reihen L und $\log L$ bei unbegrenzter Annäherung des Exponenten s an den Werth 1. Wir bemerken zunächst, dass diese Reihen je nach der Wahl der in dem Ausdrucke $\psi(n)$ vorkommenden Einheits-Wurzeln $\theta, \eta, \omega, \omega' \ldots$ ein ganz verschiedenes Verhalten zeigen; da diese Wurzeln resp. $a, b, c, c' \ldots$ verschiedene Werthe haben können, so sind in der Form L im Ganzen

$$a\,b\,c\,c' \ldots = \varphi(k)$$

verschiedene besondere Reihen enthalten; wir theilen diese Reihen L in drei Classen ein:

In die *erste* Classe nehmen wir nur eine einzige Reihe L_1 auf, und zwar diejenige, in welcher alle Einheits-Wurzeln $\theta, \eta, \omega, \omega' \ldots$ den Werth $+1$ haben.

In die *zweite* Classe nehmen wir alle übrigen Reihen L_2 auf, in welchen alle Einheits-Wurzeln reelle Werthe, also die Werthe ± 1 haben.

In die *dritte* Classe nehmen wir alle übrigen Reihen L_3 auf, d. h. alle diejenigen, in welchen wenigstens eine der Einheits-Wurzeln imaginär ist. Die Anzahl dieser Reihen ist jedenfalls gerade, und sie sind paarweise mit einander conjugirt; denn entspricht eine solche Reihe L_3 den Wurzeln $\theta, \eta, \omega, \omega' \ldots$, so entspricht immer eine zweite solche Reihe L'_3 den Wurzeln θ^{-1}, $\eta^{-1}, \omega^{-1}, \omega'^{-1} \ldots$, und diese beiden Systeme von Wurzeln sind nicht identisch.

Wir wollen nun das Verhalten aller dieser Reihen genau untersuchen, wenn der Exponent $s = 1 + \varrho$ sich dem Werthe 1 nähert, d. h. also, wenn die positive Grösse ϱ unendlich klein wird.

§. 134.

Betrachten wir zunächst das Verhalten der ersten Reihe

$$L_1 = \Sigma \frac{1}{n^s} = \Sigma \frac{1}{n^{1+\varrho}},$$

in welcher n alle relativen Primzahlen zu k durchlaufen muss, so leuchtet ein, dass dieselbe als ein Aggregat von $\varphi(k)$ Partialreihen von der Form

$$\frac{1}{\nu^{1+\varrho}} + \frac{1}{(\nu+k)^{1+\varrho}} + \frac{1}{(\nu+2k)^{1+\varrho}} + \cdots$$

angesehen werden kann, wo ν relative Primzahl zu k und $\leqq k$ ist. Da nun (nach §. 117) das Product aus einer solchen Reihe und aus ϱ mit unendlich abnehmendem ϱ sich einem endlichen positiven, von Null verschiedenen Grenzwerth k^{-1} nähert, so können wir

$$L_1 = \frac{l}{\varrho}$$

setzen, wo l mit unendlich abnehmendem ϱ sich ebenfalls einem endlichen, positiven, von Null verschiedenen Grenzwerth nähert.

Ganz anders verhalten sich aber die Reihen L der zweiten und dritten Classe; wir haben gesehen, dass alle diese Reihen, so lange $s > 1$ ist, bestimmte von der Anordnung ihrer Glieder unabhängige Werthe besitzen; von jetzt an wollen wir aber ihre Glieder $\psi(n)$ so anordnen, dass die Zahlen n ihrer Grösse nach wachsend auf einander folgen; die so geordneten Reihen L der zweiten und dritten Classe *convergiren* dann für *alle positiven* Werthe von s und sind nebst ihren Derivirten auch *stetige* Functionen des positiven Exponenten s.

Um dies nachzuweisen, betrachten wir zunächst die ganze rationale Function

$$f(x) = \Sigma\, \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots x^\nu$$

der Variabeln x, wo das Summenzeichen sich auf diejenigen $\varphi(k)$ positiven ganzen Zahlen ν bezieht, die relative Primzahlen zu k und $< k$ sind, und wo $\alpha, \beta, \gamma, \gamma' \ldots$ die Indices der Zahl ν bedeuten. Setzt man $x = 1$, so erhält man

$$f(1) = \Sigma\, \theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots,$$

wo die Indices $\alpha, \beta, \gamma, \gamma' \ldots$ unabhängig von einander vollständige Restsysteme resp. in Bezug auf die Moduln $a, b, c, c' \ldots$ durchlaufen müssen; es ist daher

$$f(1) = \Sigma\, \theta^{\alpha} . \Sigma\, \eta^{\beta} . \Sigma\, \omega^{\gamma} . \Sigma\, \omega'^{\gamma'} \ldots$$

Da nun nach unserer Voraussetzung die Reihe L eine Reihe der zweiten oder dritten Classe und folglich mindestens eine der Einheitswurzeln $\theta, \eta, \omega, \omega' \ldots$ *nicht* $= + 1$ ist, so ist auch mindestens eine der Summen

$$\Sigma\, \theta^{\alpha},\ \Sigma\, \eta^{\beta},\ \Sigma\, \omega^{\gamma},\ \Sigma\, \omega'^{\gamma'} \ldots$$

gleich Null, und hieraus folgt

$$f(1) = 0.$$

Mit Hülfe dieses Resultates kann man nun die oben behaupteten Eigenschaften der Reihen L auf verschiedene Arten nachweisen. Die eine besteht darin, dass man die Reihe L in ein bestimmtes Integral verwandelt. Nach der von *Legendre* eingeführten Bezeichnung ist

$$\Gamma(s) = \int_0^1 \left(\log \frac{1}{x}\right)^{s-1} dx$$

eine für alle positiven Werthe von s endliche und stetige Function von s; bedeutet ferner n irgend einen positiven Werth, und ersetzt man x durch x^n, so ergiebt sich

$$\frac{\Gamma(s)}{n^s} = \int_0^1 x^{n-1} \left(\log \frac{1}{x}\right)^{s-1} dx;$$

und hieraus folgt leicht (ähnlich wie in den §§. 103, 105), dass die Summe der *ersten* $m\varphi(k)$ Glieder der Reihe L gleich

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{1}{x}\, \frac{f(x)}{1 - x^k} \left(\log \frac{1}{x}\right)^{s-1} (1 - x^{mk})\, dx$$

ist. Da nun $f(x)$ eine durch x theilbare ganze Function von x ist, welche für $x = 1$ verschwindet, so bleibt innerhalb des ganzen Integrationsgebietes der Modulus der Function

$$\frac{1}{x}\, \frac{f(x)}{1 - x^k}$$

unterhalb einer angebbaren endlichen Grösse, und hieraus folgt leicht, wenn man m unendlich wachsen lässt, dass

$$L = \frac{1}{\Gamma(s)} \int_0^1 \frac{1}{x} \frac{f(x)}{1-x^k} \left(\log \frac{1}{x}\right)^{s-1} dx$$

ist. Es zeigt sich also in der That, dass die unendliche Reihe L der zweiten oder dritten Classe, wenn ihre Glieder in der angegebenen Weise geordnet sind, für jeden positiven Werth von s *convergirt*; beachtet man ferner, dass $\Gamma(s)$ für alle positiven Werthe von s ebenfalls positiv und von Null verschieden, sowie, dass die Derivirte von $\Gamma(s)$ eine stetige Function von s ist, so folgt aus dem vorstehenden geschlossenen Ausdruck für die Reihe L, dass dieselbe nebst ihrer Derivirten eine *stetige* Function von s ist, so lange s positiv bleibt.

Zu demselben Resultate gelangt man aber auch auf anderm Wege, nämlich mit Hülfe des weiter unten in §. 143 bewiesenen allgemeinen Satzes. Denn da zufolge der Gleichung $f(1) = 0$ die Summe der Coefficienten

$$\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots$$

von je $\varphi(k)$ auf einander folgenden Gliedern der Reihe L den Werth Null hat, so bildet die Reihe L eine solche unendliche Reihe, wie sie in §. 143 betrachtet wird; man braucht dort nur unter $k_1, k_2, k_3 \ldots$ die Werthe der successiven Zahlen n zu verstehen, so ergeben sich unmittelbar unsere obigen Behauptungen über die Convergenz und Stetigkeit der Reihe L und ihrer Derivirten.

Aus diesem Resultat ergiebt sich nun, dass jede Reihe L der zweiten oder dritten Classe, wenn der Exponent $s = 1 + \varrho$ abnehmend dem Werth 1 unendlich nahe kommt, sich einem völlig bestimmten *endlichen* Grenzwerth, nämlich dem Werth

$$\int_0^1 \frac{1}{x} \frac{f(x)}{1-x^k} dx$$

nähert, welchen die Reihe L bei der oben angegebenen Anordnung ihrer Glieder für $s = 1$ annimmt.

§. 135.

Es hat nun zwar gar keine Schwierigkeit, den Werth des vorstehenden Integrals mit Hülfe von Logarithmen und Kreisfunctionen darzustellen*); dass aber dieser endliche Grenzwerth einer Reihe L der zweiten oder dritten Classe *von Null verschieden* ist — und gerade hierin besteht der Hauptpunct der ganzen nachfolgenden Untersuchung — würde sich aus diesem Ausdrucke schwer oder gar nicht erkennen lassen. Es ist nun von dem höchsten Interesse, dass dieser Nachweis für die Reihen L_2 der zweiten Classe sich mit Hülfe der Untersuchungen des fünften Abschnitts über die Classenanzahl der quadratischen Formen führen lässt; ja wir können hinzufügen, dass historisch jene Untersuchungen ihren Ausgangspunct an dieser Stelle genommen haben.

Wir betrachten eine bestimmte Reihe L_2 der zweiten Classe, welche den Wurzeln

$$\theta = \pm 1, \quad \eta = \pm 1, \quad \omega = \pm 1, \quad \omega' = \pm 1 \ldots$$

entspricht; es sei P das Product aller der in k aufgehenden ungeraden Primzahlen p, denen eine negative Wurzel $\omega = -1$ entspricht, und S das Product der übrigen in k aufgehenden ungeraden Primzahlen (falls in der einen oder andern dieser beiden Gruppen gar keine Primzahl enthalten sein sollte, ist P oder $S = 1$ zu setzen); da nun eine Zahl n quadratischer Rest oder Nichtrest einer Primzahl ist, je nachdem ihr Index γ gerade oder ungerade ist (§. 129), so leuchtet ein, dass

$$\omega^{\gamma}\, \omega'^{\gamma'} \ldots = \left(\frac{n}{P}\right)$$

ist; wenn ferner $\theta = -1$, also $a = 2$, und $k \equiv 0 \pmod{4}$ ist, so sind alle Zahlen n ungerade, und es ist (nach §. 130)

$$\theta^{\alpha} = (-1)^{\alpha} = (-1)^{\frac{1}{2}(n-1)};$$

---

*) Bei der wirklichen Ausführung der Rechnung durch Zerlegung in Partialbrüche (ähnlich wie in den §§. 103, 105) würde man auf die in der Theorie der Kreistheilung vorkommenden Summen $f(r)$ stossen, wo r irgend eine Wurzel der Gleichung $r^k = 1$ bedeutet.

ebenso, wenn $\eta = -1$, also $b > 1$, und $k \equiv 0 \pmod{8}$ ist, so sind alle Zahlen n ungerade, und es ist (nach §. 130)

$$\eta^\beta = (-1)^\beta = (-1)^{1/8(n^2-1)}.$$

Diese Bemerkungen veranlassen uns (vergl. §§. 101, 123), je nach den vier verschiedenen Zeichencombinationen θ, η vier verschiedene Determinanten D zu betrachten; wir setzen nämlich, mit gehöriger Rücksicht auf das Zeichen ± 1:

$$\begin{array}{llll} D = \pm\ PS^2 \equiv 1 \pmod{4}, & \text{wenn} & \theta = +1, & \eta = +1 \\ D = \pm\ PS^2 \equiv 3 \pmod{4}, & \text{wenn} & \theta = -1, & \eta = +1 \\ D = \pm 2PS^2 \equiv 2 \pmod{8}, & \text{wenn} & \theta = +1, & \eta = -1 \\ D = \pm 2PS^2 \equiv 6 \pmod{8}, & \text{wenn} & \theta = -1, & \eta = -1. \end{array}$$

Nun sind alle ungeraden Zahlen n auch relative Primzahlen zu $2D$, und umgekehrt, alle relativen Primzahlen zu $2D$ sind auch ungerade Zahlen n, und gleichzeitig ist

$$\theta^\alpha \eta^\beta \omega^\gamma \omega'^{\gamma'} \ldots = \theta^{1/2(n-1)} \eta^{1/8(n^2-1)} \left(\frac{n}{P}\right) = \left(\frac{D}{n}\right);$$

ist daher k gerade, so stimmen die sämmtlichen Zahlen n mit den sämmtlichen relativen Primzahlen zu $2D$ überein, und es ist

$$L_2 = \Sigma\, \psi(n) = \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s};$$

ist aber k ungerade, so sind unter den Zahlen n auch gerade Zahlen; da in diesem Falle aber nothwendig $\theta = +1$, $\eta = +1$, also $D \equiv 1 \pmod{4}$ ist, so ist (vergl. §. 102)

$$L_2 = \Sigma \left(\frac{n}{P}\right) \frac{1}{n^s} = \frac{1}{1 - \left(\frac{2}{P}\right) \frac{1}{2^s}}\, \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s},$$

wo in der letzten Summe rechter Hand der Buchstabe n nur noch alle ungeraden relativen Primzahlen zu k, d. h. alle relativen Primzahlen zu $2D$ zu durchlaufen hat.

Um daher zu beweisen, dass die Reihe L_2 sich einem von Null verschiedenen Grenzwerth nähert, braucht man dasselbe nur von der Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

nachzuweisen. Nun leuchtet ein, dass die Zahl D nie eine *Quadratzahl* sein kann; denn da eine Quadratzahl niemals $\equiv 3 \pmod{4}$,

oder $\equiv 2$ (mod. 8) oder $\equiv 6$ (mod. 8) ist, so bleibt nur die einzige Möglichkeit $D \equiv 1$ (mod. 4); da aber in diesem Falle $\theta = +1$, $\eta = +1$ ist, so muss, da L_2 eine Reihe der zweiten Classe ist, wenigstens eine der Wurzeln $\omega, \omega' \ldots = -1$ sein, und folglich P mindestens durch eine ungerade Primzahl p theilbar, also nicht $= 1$ sein; mithin ist D in keinem Falle eine Quadratzahl. Wir haben nun (in §§. 96 und 98) gesehen, dass die Anzahl h der Classen nicht äquivalenter ursprünglicher Formen von der (nicht quadratischen) Determinante D ein Product aus mehreren Factoren ist, von denen der eine der Grenzwerth der obigen Reihe

$$\Sigma \left(\frac{D}{n}\right) \frac{1}{n^s}$$

ist; da nun immer mindestens eine Form $(1, 0, -D)$ existirt, also h niemals $= 0$ ist, und da ferner die übrigen in dem Ausdruck von h vorkommenden Factoren nicht unendlich gross sind, so ist auch dieser Grenzwerth von Null verschieden. Und hieraus folgt, dass auch der Grenzwerth einer jeden Reihe L_2 der zweiten Classe ein von Null verschiedener und folglich positiver Werth ist, was zu beweisen war.

In dem einfachsten Falle, wo k eine Potenz einer ungeraden Primzahl p oder das Doppelte einer solchen Potenz ist, existirt nur eine Reihe

$$L_2 = \Sigma \left(\frac{n}{p}\right) \frac{1}{n^s}$$

der zweiten Classe; in diesem Falle bedarf es nicht der Zuziehung der Theorie der quadratischen Formen, um nachzuweisen, dass der Grenzwerth

$$\Sigma \left(\frac{n}{p}\right) \frac{1}{n}$$

dieser Reihe von Null verschieden ist; für diese Summe haben wir nämlich in §. 103 einen Ausdruck gefunden, welcher neben solchen Factoren, die offenbar von Null verschieden sind, noch den Factor

$$\Sigma \left(\frac{m}{p}\right) m \quad \text{oder} \quad \Sigma \left(\frac{m}{p}\right) \log \sin \frac{m\pi}{p}$$

enthält, je nachdem $p \equiv 3$ oder $\equiv 1$ (mod. 4) ist, und wo m alle Zahlen 1, 2, 3 ... $(p-1)$ durchlaufen muss. Im ersten Fall ist aber Σm und folglich auch

$$\Sigma \left(\frac{m}{p}\right) m$$

ungerade, also von Null verschieden; im zweiten Fall ist (§. 107)

$$-\Sigma \left(\frac{m}{p}\right) \log \sin \frac{m\pi}{p} = \log \frac{y + z\sqrt{p}}{y - z\sqrt{p}},$$

wo die ganzen Zahlen y, z der Gleichung $y^2 - pz^2 = 4p$ genügen; es kann folglich z, und also auch der vorstehende Ausdruck nicht $= 0$ sein.

§. 136.

Um nun dasselbe auch für jede Reihe L_3 der dritten Classe zu beweisen, addiren wir alle $\varphi(k)$ Gleichungen von der Form

$$\Sigma \psi(q) + \tfrac{1}{2} \Sigma \psi(q^2) + \tfrac{1}{3} \Sigma \psi(q^3) + \cdots = \log L,$$

welche den verschiedenen Wurzel-Systemen θ, η, ω, ω' ... entsprechen. Bedeutet q irgend eine in k nicht aufgehende Primzahl, und μ irgend eine positive ganze Zahl, so liefert die linke Seite einer jeden solchen Gleichung ein Glied

$$\frac{1}{\mu} \psi(q^\mu),$$

in welchem

$$\frac{1}{\mu} \frac{1}{q^{\mu s}}$$

mit dem Coefficienten

$$\theta^{\alpha\mu} \eta^{\beta\mu} \omega^{\gamma\mu} \omega'^{\gamma'\mu} \ldots$$

behaftet ist, wo α, β, γ, γ' ... die Indices von q bedeuten. Die Summe aller dieser den verschiedenen Wurzelsystemen θ, η, ω, ω' ... entsprechenden Coefficienten wird daher gleich dem Product

$$\Sigma\, \theta^{\alpha\mu}\, \Sigma\, \eta^{\beta\mu}\, \Sigma\, \omega^{\gamma\mu}\, \Sigma\, \omega'^{\gamma'\mu} \ldots,$$

wo die Summenzeichen sich der Reihe nach auf die a, b, c, c' ... verschiedenen Werthe von θ, η, ω, ω' ... beziehen. Bekanntlich ist nun die Summe aller gleich hohen Potenzen der Wurzeln von einer Gleichung der Form $x^m = 1$ nur dann von Null verschieden,

und zwar $= m$, wenn der Exponent dieser Potenzen durch m theilbar ist; mithin ist das vorstehende Product nur dann von Null verschieden, und zwar $= abcc' \ldots = \varphi(k)$, wenn die Exponenten $\alpha\mu$, $\beta\mu$, $\gamma\mu$, $\gamma'\mu \ldots$ resp. durch $a, b, c, c' \ldots$ theilbar sind; da nun $\alpha\mu$, $\beta\mu$, $\gamma\mu$, $\gamma'\mu \ldots$ die Indices von q^μ sind, so wird dies nur dann und immer dann eintreten, wenn

$$q^\mu \equiv 1 \pmod{2^\lambda}, \quad q^\mu \equiv 1 \pmod{p^\pi}, \quad q^\mu \equiv 1 \pmod{p'^{\pi'}} \ldots,$$

d. h. also, wenn

$$q^\mu \equiv 1 \pmod{k}$$

ist. Mithin wird die Summe aller jener Gleichungen folgende Form annehmen

$$\varphi(k)\left\{\Sigma \frac{1}{q^s} + \tfrac{1}{2}\Sigma \frac{1}{q^{2s}} + \cdots + \frac{1}{\mu}\Sigma \frac{1}{q^{\mu s}} + \cdots\right\}$$
$$= \log L_1 + \Sigma \log L_2 + \Sigma \log(L_3 L'_3),$$

wo auf der linken Seite das erste, zweite Summenzeichen u. s. f. sich auf alle die in k nicht aufgehenden Primzahlen q bezieht, welche resp. den Bedingungen $q \equiv 1$, $q^2 \equiv 1 \pmod{k}$ u. s. f. Genüge leisten; auf der rechten Seite bezieht sich das erste Summenzeichen auf alle Reihen L_2 der zweiten Classe, das zweite auf alle verschiedenen Paare $L_3 L'_3$ conjugirter Reihen dritter Classe. Mit Hülfe dieser Gleichung sind wir im Stande zu beweisen, dass der endliche Grenzwerth, welchem sich irgend eine Reihe L_3 der dritten Classe nähert, von Null verschieden ist.

Dieser Beweis stützt sich auf das schon früher (§. 134) erhaltene Resultat, dass jede solche Reihe L_3 für alle positiven Werthe von s eine stetige Function von s ist, und dass dasselbe auch von ihrer Derivirten gilt. Wir können daher

$$L_3 = f(s) + iF(s)$$
$$L'_3 = f(s) - iF(s)$$

setzen, wo $f(s)$, $F(s)$ und die Derivirten $f'(s)$, $F'(s)$ stetige Functionen von s sind, so lange s positiv bleibt; da also der Grenzwerth von $L_3 = f(1) + iF(1)$ ist, so muss, falls derselbe $= 0$ ist, nothwendig $f(1) = 0$ und $F(1) = 0$ sein; hieraus folgt nach einem bekannten Satze der Differentialrechnung, dass für jeden Werth $s = 1 + \varrho$, welcher > 1 ist,

$$L_3 = \varrho \,\{f'(1+\delta\varrho) + iF'(1+\varepsilon\varrho)\}$$
$$L'_3 = \varrho \,\{f'(1+\delta\varrho) - iF'(1+\varepsilon\varrho)\}$$

sein wird, wo δ und ε zwischen den Grenzen 0 und 1 liegen; mithin wird

$$L_3 L'_3 = \varrho^2 \,\{f'(1+\delta\varrho)^2 + F'(1+\varepsilon\varrho)^2\} = \varrho^2 R,$$

wo R (in Folge der Endlichkeit und Stetigkeit der Derivirten $f'(s)$, $F'(s)$) mit unendlich abnehmendem positiven ϱ sich einem endlichen (nicht negativen) Grenzwerth

$$f'(1)^2 + F'(1)^2$$

nähert. Hieraus folgt nun

$$\log(L_3 L'_3) = -2 \log \frac{1}{\varrho} + \log R,$$

wo $\log R$ mit unendlich abnehmendem ϱ sich entweder einem endlichen Grenzwerth nähert oder negativ über alle Grenzen wächst, falls R unendlich klein wird.

Sind im Ganzen m solche Paare von Reihen dritter Classe vorhanden, welche gleichzeitig mit ϱ unendlich klein werden, so ist folglich

$$\Sigma \log(L_3 L'_3) = -2m \log \frac{1}{\varrho} + t,$$

wo t jedenfalls nicht positiv über alle Grenzen wachsen kann, sondern entweder endlich bleibt, oder negativ über alle Grenzen wächst; denn da jedes Product $L_3 L'_3$ sich einem endlichen nicht negativen Werth nähert, so kann auch kein Glied $\log(L_3 L'_3)$ positiv über alle Grenzen wachsen.

Da ferner schon gezeigt ist, dass der Grenzwerth einer jeden Reihe L_2 der zweiten Classe von Null verschieden ist, so nähert sich die Summe

$$\Sigma \log L_2$$

der (jedenfalls reellen) Reihen $\log L_2$ einem endlichen Grenzwerth.

Ausserdem ist schon bewiesen, dass das Product ϱL_1 sich einem endlichen von Null verschiedenen Werth nähert; mithin ist

$$\log L_1 = \log \frac{1}{\varrho} + t',$$

wo t' endlich bleibt; folglich ist die ganze rechte Seite der obigen Gleichung von der Form

$$-(2m-1)\log\frac{1}{\varrho}+T,$$

wo T mit unendlich abnehmendem ϱ jedenfalls nicht positiv über alle Grenzen wachsen kann. Existirte also mindestens eine Reihe L_3 dritter Classe, welche mit ϱ unendlich klein würde, d. h. wäre m mindestens $=1$, so würde die ganze rechte Seite unserer Gleichung mit unendlich abnehmendem positiven ϱ *negativ* unendlich wachsen. Dies ist aber unmöglich, da die linke Seite für alle Werthe von ϱ positiv bleibt. Mithin ist $m=0$, d. h. jede Reihe der dritten Classe nähert sich einem von Null verschiedenen Grenzwerth, was zu beweisen war.

Hieraus folgt endlich noch, dass auch jede der Reihen $\log L_3$ einen endlichen Grenzwerth haben muss, wenn man berücksichtigt, dass nach dem früher Bewiesenen (§. 133) jede solche Reihe sich stetig mit s ändert, so lange $s>1$ ist.

§. 137.

Das Resultat der vorhergehenden Untersuchungen besteht darin, dass bei dem unendlichen Abnehmen der positiven Grösse $\varrho=s-1$ die Reihe $\log L_1$ positiv über alle Grenzen wächst, während alle übrigen Reihen $\log L$ sich endlichen Grenzwerthen nähern. Mit Hülfe desselben sind wir im Stande, den Satz über die arithmetische Progression vollständig zu beweisen.

Es sei nämlich m irgend eine relative Primzahl zu k, so multipliciren wir jede der $\varphi(k)$ Reihen von der Form

$$\Sigma\,\psi(q)+\tfrac{1}{2}\,\Sigma\,\psi(q^2)+\tfrac{1}{3}\,\Sigma\,\psi(q^3)+\cdots=\log L,$$

welche einem bestimmten System von Einheits-Wurzeln $\theta,\eta,\omega,\omega'\ldots$ entspricht, mit dem correspondirenden Werth

$$\theta^{-\alpha_1}\eta^{-\beta_1}\omega^{-\gamma_1}\omega'^{-\gamma_1'}\ldots=\chi,$$

wo $\alpha_1,\beta_1,\gamma_1,\gamma_1'\ldots$ die Indices der Zahl m bedeuten, und addiren alle Producte; dann wird, wenn wieder $\alpha,\beta,\gamma,\gamma'\ldots$ die Indices einer bestimmten Primzahl q sind, das Glied

$$\frac{1}{\mu}\,\frac{1}{q^{\mu s}}$$

den Coefficienten

$$\sum \theta^{\alpha\mu-\alpha_1}\eta^{\beta\mu-\beta_1}\omega^{\gamma\mu-\gamma_1}\omega'^{\gamma'\mu-\gamma_1'}\ldots$$

erhalten, wo sich das Summenzeichen auf alle $\varphi(k)$ Wurzel-Systeme bezieht; dieser Coefficient ist daher auch gleich dem Product aus den einzelnen Summen

$$\sum \theta^{\alpha\mu-\alpha_1},\ \sum \eta^{\beta\mu-\beta_1},\ \sum \omega^{\gamma\mu-\gamma_1},\ \sum \omega'^{\gamma'\mu-\gamma_1'}\ldots,$$

in welchen die Buchstaben $\theta, \eta, \omega, \omega' \ldots$ resp. ihre $a, b, c, c' \ldots$ verschiedenen Werthe durchlaufen müssen; dieser Coefficient wird folglich nur dann von Null verschieden, und zwar $= abcc' \ldots = \varphi(k)$ sein, wenn die Exponenten $\alpha\mu - \alpha_1$, $\beta\mu - \beta_1$, $\gamma\mu - \gamma_1$, $\gamma'\mu - \gamma_1' \ldots$ resp. durch $a, b, c, c' \ldots$ theilbar sind, d. h. wenn

$$q^{\mu} \equiv m \pmod{k}$$

ist. Die Summation aller Producte $\chi \log L$ giebt daher das Resultat

$$\varphi(k)\left\{\sum \frac{1}{q^s} + \tfrac{1}{2}\sum \frac{1}{q^{2s}} + \tfrac{1}{3}\sum \frac{1}{q^{3s}} + \cdots\right\} = \sum \chi \log L,$$

wo auf der linken Seite das erste, zweite, dritte Summenzeichen u. s. f. sich auf alle Primzahlen q bezieht, welche resp. den Bedingungen $q \equiv m$, $q^2 \equiv m$, $q^3 \equiv m \pmod{k}$ u. s. f. genügen, während das Summenzeichen auf der rechten Seite sich auf die sämmtlichen $\varphi(k)$ verschiedenen Wurzel-Systeme $\theta, \eta, \omega, \omega' \ldots$ bezieht. Bezeichnet man nun mit z alle positiven ganzen Zahlen mit Ausnahme von 1, so ist offenbar

$$\tfrac{1}{2}\sum \frac{1}{q^{2s}} + \tfrac{1}{3}\sum \frac{1}{q^{3s}} + \tfrac{1}{4}\sum \frac{1}{q^{4s}} + \cdots = Q$$

kleiner als

$$\tfrac{1}{2}\sum \frac{1}{z^2} + \tfrac{1}{2}\sum \frac{1}{z^3} + \tfrac{1}{2}\sum \frac{1}{z^4} + \cdots,$$

wo in jeder Summe z alle seine Werthe durchläuft; da nun, sobald $z \geqq 2$, immer

$$\frac{1}{z^3} \leqq \frac{1}{2}\frac{1}{z^2},\quad \frac{1}{z^4} \leqq \frac{1}{4}\frac{1}{z^2},\quad \frac{1}{z^5} \leqq \frac{1}{8}\frac{1}{z^2}\ldots$$

ist, so ergiebt sich

$$Q < \sum \frac{1}{z^2};$$

während daher s abnehmend sich dem Werthe 1 nähert, bleibt Q fortwährend unterhalb einer endlichen Grösse. Da ferner alle Glieder $\chi \log L$ sich endlichen Grenzwerthen nähern, mit Ausnahme des einzigen Gliedes $\log L_1$, welches über alle Grenzen wächst, so muss auch die Summe

$$\Sigma \frac{1}{q^s}$$

über alle Grenzen wachsen; dies wäre aber nicht möglich, wenn diese Summe aus einer endlichen Anzahl von Gliedern bestände, und folglich muss es unendlich viele Primzahlen q geben, welche $\equiv m \pmod{k}$ sind; d. h. also:

Jede unbegrenzte arithmetische Progression $kx + m$, deren Anfangsglied m und Differenz k relative Primzahlen sind, enthält unendlich viele positive Primzahlen q *).

*) Ueber die Ausdehnung dieses Satzes auf Linearformen mit complexen Coefficienten, sowie auf quadratische Formen siehe *Dirichlet: Untersuchungen über die Theorie der complexen Zahlen*, Abhandlungen der Berliner Akademie aus dem Jahre 1841; Monatsbericht der Berliner Akademie (März 1840) oder Crelle's Journal XXI; Comptes rendus der Pariser Akademie 1849, T. X, p. 285.

VII. Ueber einige Sätze aus der Theorie der Kreistheilung.

§. 138.

Sind $p, p', p'' \ldots$ positive und von einander verschiedene Primzahlen, so stimmen (nach §. 9) die Glieder des entwickelten Productes

$$(p+1)(p'+1)(p''+1)\ldots$$

mit den sämmtlichen Divisoren des Productes

$$P = pp'p'' \ldots$$

überein; dieselben Divisoren entstehen offenbar auch durch die Entwicklung des Productes

$$(p-1)(p'-1)(p''-1)\ldots,$$

aber die eine Hälfte derselben wird mit positivem, die andere mit negativem Zeichen behaftet sein; wir wollen die erstern mit δ_1, die letztern mit δ_2 bezeichnen, so dass

$$(p-1)(p'-1)(p''-1)\ldots = \Sigma\,\delta_1 - \Sigma\,\delta_2$$

wird, und wir bemerken, dass die Zahl P selbst zu der Classe der erstern gehört. Ist nun δ irgend ein Divisor von P, aber $< P$, so lässt sich leicht zeigen, dass die Anzahl der durch δ theilbaren Zahlen δ_1 genau gleich der Anzahl der durch δ theilbaren Zahlen δ_2 ist. Denn wenn man mit $q, q', q'' \ldots$ alle diejenigen Primfactoren von P bezeichnet, welche nicht in δ aufgehen, so stimmen die durch δ theilbaren Zahlen δ_1 und $-\delta_2$ resp. mit den positiven und negativen Gliedern des entwickelten Productes

$$\delta(q-1)(q'-1)(q''-1)\ldots$$

überein, und da $\delta < P$ ist, also mindestens eine solche Primzahl q vorhanden ist, so ist die Anzahl der positiven Glieder dieses Productes genau gleich der Anzahl der negativen.

Dieser Satz lässt sich leicht verallgemeinern. Bedeutet m irgend eine positive ganze Zahl > 1, und sind $p, p', p'' \ldots$ die sämmtlichen von einander verschiedenen in m aufgehenden positiven Primzahlen, so kann man

$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{p''}\right)\cdots = \Sigma\,\mu_1 - \Sigma\,\mu_2$$

setzen, wo mit μ_1 und $-\mu_2$ resp. alle positiven und negativen Glieder des entwickelten Productes linker Hand bezeichnet sind. Behält man die vorhergehenden Bezeichnungen bei, so stimmen offenbar die Zahlen μ_1 und μ_2 resp. mit den Zahlen $m'\delta_1$ und $m'\delta_2$ überein, wenn zur Abkürzung $m = m'P$ gesetzt wird. Bedeutet nun μ irgend einen Divisor von m, mit Ausnahme von m selbst, so folgt hieraus wieder, dass unter den Zahlen μ_1 ebenso viele durch μ theilbar sein werden, wie unter den Zahlen μ_2. Denn, wenn μ' der grösste gemeinschaftliche Divisor von μ und m' ist, so kann man $\mu = \mu'\delta$ setzen, wo δ nothwendig ein Divisor von P, und zwar $< P$ sein muss; und da eine Zahl $\mu_1 = m'\delta_1$ oder $\mu_2 = m'\delta_2$ stets und nur dann durch $\mu = \mu'\delta$ theilbar ist, sobald resp. δ_1 oder δ_2 durch δ theilbar ist, so ergiebt sich in der That, dass die Anzahl der durch μ theilbaren Zahlen μ_1 genau gleich der Anzahl der durch μ theilbaren Zahlen μ_2 ist.

Von dieser Eigenschaft der Zahlen μ_1 und μ_2 kann man vielfache Anwendungen machen. Hängen z. B. zwei Functionen $f(m)$ und $F(m)$ einer beliebigen ganzen Zahl m durch eine der beiden Relationen

$$\Sigma f(\mu) = F(m)$$

oder

$$\Pi f(\mu) = F(m)$$

zusammen, wo das Summen- oder Productzeichen sich jedesmal auf alle Divisoren μ (incl. m) der Zahl m bezieht, so folgt daraus resp. die Umkehrung

$$f(m) = \Sigma\,F(\mu_1) - \Sigma\,F(\mu_2)$$

oder

$$f(m) = \frac{\Pi\,F(\mu_1)}{\Pi\,F(\mu_2)},$$

wo die Summen- oder Productzeichen sich auf alle Werthe von μ_1 oder auf alle Werthe von μ_2 beziehen; denn ersetzt man rechts jeden Werth $F(\mu_1)$ und $F(\mu_2)$ durch die Summe oder das Product der Werthe $f(\mu)$, die den sämmtlichen Divisoren μ von μ_1 oder μ_2 entsprechen, so werden zufolge der obigen Eigenschaft der Zahlen μ_1, μ_2 alle Werthe $f(\mu)$ sich aufheben, in welchen $\mu < m$ ist, und es wird allein der Werth $f(m)$ zurückbleiben.

Als Beispiel wählen wir die Aufgabe, die Anzahl $\varphi(m)$ der ganzen Zahlen zu bestimmen, welche relative Primzahlen zu m und nicht grösser als m sind; aus dieser Definition der Function $\varphi(m)$ ist in §. 13 ohne alle Rechnung der Satz abgeleitet, dass

$$\Sigma\, \varphi(\mu) = m$$

ist, wo das Summenzeichen sich auf alle Divisoren μ von m bezieht; setzen wir daher $F(m) = m$, so ergiebt sich umgekehrt

$$\varphi(m) = \Sigma\, \mu_1 - \Sigma\, \mu_2,$$

also

$$\varphi(m) = m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{p''}\right)\cdots;$$

diese Function ist daher durch den Satz des §. 13 schon vollständig charakterisirt.

Ein anderes Beispiel ist folgendes. Ist der Werth der Function $f(m) = p$, sobald die Zahl m eine Potenz einer Primzahl p ist, dagegen $= 1$, so oft $m = 1$ oder durch mehrere verschiedene Primzahlen theilbar ist, so leuchtet ein, dass

$$\Pi\, f(\mu) = m$$

ist, wo das Productzeichen sich auf alle Divisoren μ von m bezieht; hieraus folgt nach dem obigen Satze, dass umgekehrt der Quotient

$$\frac{\Pi\, \mu_1}{\Pi\, \mu_2} = f(m),$$

also nur dann von 1 verschieden ist, wenn m eine Potenz einer Primzahl ist; und zwar ist dieser Quotient dann gleich dieser Primzahl.

Aus der Definition der Divisoren μ_1 und μ_2 folgt endlich auch, dass stets

$$\psi(m)\,(\psi(p)-1)\,(\psi(p')-1)\,(\psi(p'')-1)\ldots = \Sigma\,\psi(\mu_1) - \Sigma\,\psi(\mu_2)$$

ist, wenn die Function ψ die Eigenschaft $\psi(z)\,\psi(z') = \psi(zz')$ besitzt.

§. 139.

Die sämmtlichen Wurzeln ϱ der Gleichung

$$x^m = 1 \tag{1}$$

sind bekanntlich in der Form enthalten

$$\varrho = \cos\frac{2n\pi}{m} + i\sin\frac{2n\pi}{m},$$

wo n irgend ein vollständiges Restsystem (mod. m) durchlaufen muss.

Ist n relative Primzahl zu m, so sind die Potenzen

$$1,\ \varrho,\ \varrho^2 \ldots \varrho^{m-1}$$

sämmtlich ungleich, und sie bilden die sämmtlichen Wurzeln der obigen Gleichung (1); ϱ heisst in diesem Fall eine *primitive* Wurzel dieser Gleichung, und die Anzahl dieser primitiven Wurzeln ist offenbar $= \varphi(m)$. Ist allgemeiner ν der grösste gemeinschaftliche Divisor von n und $m = \mu\nu$, so ist ϱ eine primitive Wurzel der Gleichung

$$x^\mu = 1, \tag{2}$$

und da umgekehrt jede Wurzel der letztern Gleichung (2) auch eine Wurzel der Gleichung (1) ist, so leuchtet ein, dass die sämmtlichen Wurzeln der Gleichung (1) identisch sind mit allen primitiven Wurzeln aller der Gleichungen (2), die den sämmtlichen Divisoren μ der Zahl m entsprechen. Bezeichnet man daher mit ϱ' alle $\varphi(\mu)$ primitiven Wurzeln der Gleichung (2), und setzt

$$f(\mu) = \Pi\,(x - \varrho'),$$

wo das Productzeichen sich auf alle Wurzeln ϱ' bezieht, so ist

$$\Pi\, f(\mu) = x^m - 1,$$

wo das Productzeichen sich auf alle Divisoren μ der Zahl m bezieht; durch Umkehrung dieser für jede Zahl m geltenden Relation erhält man nach dem vorhergehenden Paragraphen

$$f(m) = \frac{\Pi\,(x^{\mu_1} - 1)}{\Pi\,(x^{\mu_2} - 1)},$$

woraus folgt, dass die Coefficienten der Function $f(m)$ sämmtlich ganze rationale Zahlen sind.

Von jetzt an betrachten wir nur noch den Fall, in welchem $m = P = pp'p'' \dots$ eine ungerade und durch kein Quadrat theilbare ganze Zahl > 1 ist. Dann wird

$$\varphi(P) = (p-1)(p'-1)(p''-1)\dots = \Sigma\, \mu_1 - \Sigma\, \mu_2$$

eine gerade Zahl, die wir mit 2τ bezeichnen wollen, und die sämmtlichen 2τ relativen Primzahlen zu P, welche $< P$ sind, zerfallen in τ Zahlen a und in τ Zahlen b von der Beschaffenheit, dass

$$\left(\frac{a}{P}\right) = +1, \quad \left(\frac{b}{P}\right) = -1$$

ist (§. 52. I. oder Supplemente §. 116). Setzen wir daher

$$\theta = \cos\frac{2\pi}{P} + i \sin\frac{2\pi}{P} = e^{\frac{2\pi i}{P}}$$

und

$$A(x) = \Pi(x - \theta^a), \quad B(x) = \Pi(x - \theta^b),$$

so wird

$$A(x)\, B(x) = \frac{\Pi(x^{\mu_1} - 1)}{\Pi(x^{\mu_2} - 1)},$$

und wir wollen im Folgenden die allgemeine Form der Coefficienten der Functionen $A(x)$, $B(x)$ bestimmen.

Zu diesem Zwecke erinnern wir zunächst an die Newton'schen Formeln, welche dazu dienen, aus den Coefficienten einer Gleichung die Summen gleich hoher Potenzen ihrer Wurzeln, und umgekehrt aus diesen jene abzuleiten. Es seien

$$w_1,\ w_2 \dots w_m$$

die Wurzeln einer Gleichung

$$x^m + c_1 x^{m-1} + c_2 x^{m-2} + \dots + c_m = 0,$$

und

$$S_k = w_1^k + w_2^k + \dots + w_m^k,$$

so lauten diese Formeln folgendermaassen:

$$\begin{aligned} &S_1 + c_1 = 0 \\ &S_2 + c_1 S_1 + 2c_2 = 0 \\ &S_3 + c_1 S_2 + c_2 S_1 + 3c_3 = 0 \\ &\dots\dots\dots\dots\dots\dots \\ &S_m + c_1 S_{m-1} + c_2 S_{m-2} + \dots + c_{m-1} S_1 + m c_m = 0. \end{aligned}$$

Aus der Form derselben geht hervor, dass $S_1, S_2 \ldots S_m$ ganze rationale Zahlen sein werden, sobald die Coefficienten $c_1, c_2 \ldots c_m$ sämmtlich ganze rationale Zahlen sind. Wenden wir dies auf die Gleichung

$$\frac{\Pi\,(x^{\mu_1}-1)}{\Pi\,(x^{\mu_2}-1)}=0$$

an, so ergiebt sich, dass

$$S_k=\Sigma\,\theta^{ak}+\Sigma\,\theta^{bk}$$

für jeden Werth $k=1, 2, 3 \ldots$ eine ganze Zahl ist. Andererseits ist nun (Supplemente §. 116)

$$\Sigma\,\theta^{ak}-\Sigma\,\theta^{bk}=\left(\frac{k}{P}\right)i^{\frac{1}{4}(P-1)^2}\sqrt{P},$$

und folglich

$$\Sigma\,\theta^{ak}=\tfrac{1}{2}\left(S_k+\left(\frac{k}{P}\right)i^{\frac{1}{4}(P-1)^2}\sqrt{P}\right)$$

$$\Sigma\,\theta^{bk}=\tfrac{1}{2}\left(S_k-\left(\frac{k}{P}\right)i^{\frac{1}{4}(P-1)^2}\sqrt{P}\right);$$

hiermit sind die Summen der $k$ten Potenzen der Wurzeln von jeder der beiden Gleichungen

$$A(x)=0,\quad B(x)=0$$

gefunden, und da dieselben keine andere Irrationalität enthalten als die Quadratwurzel

$$i^{\frac{1}{4}(P-1)^2}\sqrt{P},$$

so gilt zufolge der Newton'schen Formeln dasselbe von sämmtlichen Coefficienten dieser beiden Gleichungen, und zwar werden zwei gleich hohe Coefficienten in beiden Gleichungen sich nur durch das Vorzeichen dieser Quadratwurzel von einander unterscheiden, d. h. zwei solche Coefficienten werden die Formen

$$y-z\,i^{\frac{1}{4}(P-1)^2}\sqrt{P}\quad\text{und}\quad y+z\,i^{\frac{1}{4}(P-1)^2}\sqrt{P}$$

haben, wo y und z rationale Zahlen bedeuten. Man kann ferner behaupten, dass y und z entweder ganze Zahlen oder Brüche mit dem Nenner 2 sind, obgleich dies aus den Newton'schen Formeln nicht unmittelbar hervorgeht; um den Beweis dieser Behauptung anzudeuten, wollen wir jede Gleichung, deren höchster Coefficient $=1$, und deren übrige Coefficienten ganze rationale Zahlen sind, eine primäre Gleichung nennen; dann überzeugt man sich leicht, dass die Summe und Differenz zweier Wurzeln von primären

Gleichungen (und ebenso ihr Product) wieder Wurzeln von primären Gleichungen sind; da nun θ die Wurzel einer primären Gleichung ist, so gilt dasselbe von jedem Coefficienten der Functionen $A(x)$ und $B(x)$ und folglich auch von

$$2y \quad \text{und} \quad 2z\,i^{1/4(P-1)^2}\sqrt{P},$$

und hieraus folgt sogleich, dass die rationalen Zahlen $2y$ und $2z$ *ganze* Zahlen sein müssen.

Fasst man dies zusammen, so ergiebt sich, dass man gleichzeitig

$$2A(x) = Y(x) - Z(x)\,i^{1/4(P-1)^2}\sqrt{P}$$
$$2B(x) = Y(x) + Z(x)\,i^{1/4(P-1)^2}\sqrt{P}$$

setzen kann, wo $Y(x)$ und $Z(x)$ ganze Functionen bedeuten, deren sämmtliche Coefficienten ganze rationale Zahlen sind*). Multiplicirt man die beiden Gleichungen mit einander, so erhält man

$$Y(x)^2 - \left(\frac{-1}{P}\right) P\, Z(x)^2 = 4\,\frac{\Pi\,(x^{\mu_1}-1)}{\Pi\,(x^{\mu_2}-1)}.$$

§. 140.

Wir bemerken nun noch, dass man immer nur die Hälfte der Coefficienten von $Y(x)$ und $Z(x)$ zu berechnen braucht. Es ist nämlich

$$x^\tau A\left(\frac{1}{x}\right) = \Pi\,(1-\theta^a x) = (-1)^\tau \theta^{\Sigma a}\,\Pi\,(x-\theta^{-a})$$

$$x^\tau B\left(\frac{1}{x}\right) = \Pi\,(1-\theta^b x) = (-1)^\tau \theta^{\Sigma b}\,\Pi\,(x-\theta^{-b});$$

nun ist, je nachdem $P \equiv 1$, oder $P \equiv 3 \pmod{4}$ ist,

$$\left(\frac{-1}{P}\right) = +1, \quad \text{oder} \quad \left(\frac{-1}{P}\right) = -1,$$

und folglich

$$\Pi\,(x-\theta^{-a}) = A(x),\ \ \Pi\,(x-\theta^{-b}) = B(x)$$

oder

$$\Pi\,(x-\theta^{-a}) = B(x),\ \ \Pi\,(x-\theta^{-b}) = A(x);$$

*) Vergl. *Gauss: D. A.* art. 357.

ist ferner P nicht $= 3$, so existirt unter den Zahlen a eine Zahl a' von der Beschaffenheit, dass $(a'-1)$ relative Primzahl zu P ist, und da die Reste der Producte aa' mit den Zahlen a, und die Reste der Producte ba' mit den Zahlen b im Complex übereinstimmen, so ist

$$a' \sum a \equiv \sum a, \quad a' \sum b \equiv \sum b \pmod{P}$$

und folglich

$$\sum a \equiv 0, \quad \sum b \equiv 0 \pmod{P},$$

also

$$\theta^{\Sigma a} = 1, \quad \theta^{\Sigma b} = 1.$$

Mithin ergiebt sich (da τ gerade, sobald $P \equiv 1 \pmod{4}$)

$$\left.\begin{aligned} A(x) &= x^\tau A\left(\frac{1}{x}\right) \\ B(x) &= x^\tau B\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 1 \pmod{4}$$

und, mit Ausnahme von $P = 3$,

$$\left.\begin{aligned} A(x) &= (-x)^\tau B\left(\frac{1}{x}\right) \\ B(x) &= (-x)^\tau A\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 3 \pmod{4}$$

und hieraus

$$\left.\begin{aligned} Y(x) &= x^\tau Y\left(\frac{1}{x}\right) \\ Z(x) &= x^\tau Z\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 1 \pmod{4}$$

und, mit Ausnahme von $P = 3$,

$$\left.\begin{aligned} Y(x) &= (-x)^\tau Y\left(\frac{1}{x}\right) \\ -Z(x) &= (-x)^\tau Z\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 3 \pmod{4}$$

Diese Gleichungen enthalten Relationen zwischen je zwei gleich weit vom Anfang und Ende abstehenden Coefficienten der Functionen $Y(x)$ und $Z(x)$.

Die wirkliche Berechnung der Coefficienten der beiden Functionen

$$Y(x) = y_0 x^\tau + y_1 x^{\tau-1} + \cdots + y_\tau$$
$$Z(x) = z_0 x^\tau + z_1 x^{\tau-1} + \cdots + z_\tau$$

geschieht nun auf folgende Art. Zuerst bildet man die Potenzsummen

$$S_k = \Sigma\,\theta^{ak} + \Sigma\,\theta^{bk}$$

für $k = 1, 2, 3 \ldots$ bis zu $\frac{1}{2}\tau$ oder $\frac{1}{2}(\tau - 1)$, je nachdem τ gerade oder ungerade ist; dies kann nach dem Obigen dadurch geschehen, dass man ebenso viele Coefficienten der ganzen Function

$$\frac{\Pi\,(x^{\mu_1} - 1)}{\Pi\,(x^{\mu_2} - 1)}$$

vom höchsten an gerechnet durch wirkliche Division bestimmt, und dann die Newton'schen Formeln anwendet; indessen hält es nicht schwer, durch Betrachtungen, welche ebenfalls auf der im §. 138 bewiesenen Haupteigenschaft der Zahlen μ_1 und μ_2 beruhen, folgende Regel abzuleiten: es sei Q der grösste gemeinschaftliche Divisor von k und $P = QR$, und r die Anzahl der in R aufgehenden Primzahlen, so ist*)

$$S_k = (-1)^r \varphi(Q).$$

Nachdem diese Werthe S_k gefunden sind, erhält man die Coefficienten der Functionen $Y(x)$ und $Z(x)$ durch die beiden aus den Newton'schen Formeln abgeleiteten Recursionsgleichungen

$$2\,k y_k = \left\{ \begin{array}{c} -\Big[S_k y_0 + S_{k-1} y_1 + \cdots + S_1 y_{k-1}\Big] \\ +\left(\frac{-1}{P}\right) P \Big[\left(\frac{k}{P}\right) z_0 + \left(\frac{k-1}{P}\right) z_1 + \cdots + \left(\frac{1}{P}\right) z_{k-1}\Big] \end{array} \right\}$$

$$2\,k z_k = \left\{ \begin{array}{c} +\Big[\left(\frac{k}{P}\right) y_0 + \left(\frac{k-1}{P}\right) y_1 + \cdots + \left(\frac{1}{P}\right) y_{k-1}\Big] \\ -\Big[S_k z_0 + S_{k-1} z_1 + \cdots + S_1 z_{k-1}\Big] \end{array} \right\}$$

wenn man noch berücksichtigt, dass

$$y_0 = 2, \quad z_0 = 0$$

ist.

*) Allgemeiner lautet diese Regel so: ist $m = m'P$ eine beliebige positive ganze Zahl, P das Product aus allen von einander verschiedenen in m aufgehenden Primzahlen, und S_k die Summe der $k$ten Potenzen aller primitiven Wurzeln der Gleichung $x^m = 1$, so ist $S_k = 0$, so oft k nicht durch m' theilbar ist; ist aber $k = m'K$, ferner Q der grösste gemeinschaftliche Divisor von K und $P = QR$, und r die Anzahl der in R aufgehenden Primzahlen, so ist

$$S_k = (-1)^r\, m'\, \varphi(Q).$$

Beispiel 1: $P = 3$; in diesem Falle müssen alle Coefficienten berechnet werden; da

$$S_1 = -1, \quad \left(\frac{1}{P}\right) = 1$$

ist, so erhält man

$$2y_1 = -S_1 y_0 = 2, \quad 2z_1 = \left(\frac{1}{P}\right) y_0 = 2,$$

und folglich

$$Y(x) = 2x + 1, \quad Z(x) = 1.$$

Beispiel 2: $P = 5$; $\tau = 2$; da wieder

$$S_1 = -1, \quad \left(\frac{1}{P}\right) = 1$$

ist, so erhält man auch wieder

$$y_1 = 1, \quad z_1 =$$

und folglich

$$Y(x) = 2x^2 + x + 2, \quad Z(x) = x.$$

Beispiel 3: $P = 15 = 3.5$; $\tau = 4$; hier ist

$$S_1 = S_2 = 1; \quad \left(\frac{1}{P}\right) = \left(\frac{2}{P}\right) = 1; \quad \left(\frac{-1}{P}\right) = -1;$$

und folglich erhält man successive

$$y_1 = -1, \quad z_1 = 1$$

und

$$y_2 = -4, \quad z_2 = 0;$$

also ist

$$Y(x) = 2x^4 - x^3 - 4x^2 - x + 2, \quad Z(x) = x^3 - x.$$

VIII. Ueber die Pell'sche Gleichung.

§. 141.

Bedeutet D eine positive ganze Zahl, die aber kein vollständiges Quadrat ist, so ist in §. 83 durch die Betrachtung der Perioden von reducirten quadratischen Formen, die zur Determinante D gehören, nachgewiesen, dass die Pell'sche oder Fermat'sche Gleichung

$$t^2 - Du^2 = 1$$

immer unendlich viele Lösungen in ganzen positiven Zahlen t, u besitzt, und es ist dort auch eine Methode gegeben, durch welche alle diese Lösungen gefunden werden können. Es hat durchaus keine Schwierigkeit, den Zusammenhang zwischen allen diesen Lösungen zu finden, sobald nur erst der Hauptpunct bewiesen ist, dass wirklich eine Lösung existirt, in welcher u von Null verschieden ist (§. 85); *Lagrange* gebührt das Verdienst, durch Einführung neuer Principien in die Zahlentheorie diese Schwierigkeit zuerst vollständig überwunden zu haben, und diese Principien sind später in hohem Grade verallgemeinert*). Wir wollen deshalb hier noch einen Beweis der Lösbarkeit der Pell'schen Gleichung

---

*) Vergl. drei Abhandlungen von *Dirichlet* in den Monatsberichten der Berliner Akademie vom October 1841, April 1842, März 1846; ferner die Comptes rendus der Pariser Akademie 1840, T. X, p. 286—288. — Vergl. *P. Bachmann: De unitatum complexarum theoria.* 1864.

mittheilen, welcher im Wesentlichen auf derselben Grundlage beruht.

Das Fundament dieses Beweises beruht auf der Thatsache, dass immer unendlich viele Paare von ganzen Zahlen x, y existiren, für welche, abgesehen vom Vorzeichen,

$$x^2 - Dy^2 < 1 + 2\sqrt{D}$$

ist; man überzeugt sich hiervon leicht, wenn man aus der Theorie der Kettenbrüche den Satz entlehnt, dass jeder Näherungswerth $x:y$, den man durch Entwicklung einer Grösse ω in einen Kettenbruch erhält, um weniger als y^{-2} von ω verschieden ist; nimmt man also $\omega = \sqrt{D}$, so giebt es, da $\sqrt{D}$ irrational ist, unendlich viele solche Zahlenpaare x, y von der Beschaffenheit, dass, abgesehen vom Vorzeichen,

$$\frac{x}{y} - \sqrt{D} < \frac{1}{y^2}, \text{ also } x - y\sqrt{D} = \frac{\delta}{y}$$

ist, wo δ einen positiven oder negativen echten Bruch bedeutet; hieraus folgt

$$x + y\sqrt{D} = \frac{\delta}{y} + 2y\sqrt{D},$$

und durch Multiplication

$$x^2 - Dy^2 = \frac{\delta^2}{y^2} + 2\delta\sqrt{D} < 1 + 2\sqrt{D}.$$

Um aber Nichts aus der Theorie der Kettenbrüche zu entlehnen, wollen wir diesen Satz noch auf einem andern und zwar ganz einfachen Wege beweisen. Es sei m irgend eine positive ganze Zahl, so legen wir der Zahl y der Reihe nach die $m+1$ Werthe

$$0, 1, 2 \ldots (m-1), m$$

bei, und bestimmen für jeden dieser Werthe die zugehörige ganze Zahl x durch die Bedingung

$$0 \leqq x - y\sqrt{D} < 1,$$

welche offenbar jedesmal durch eine, und nur durch eine ganze Zahl x erfüllt wird. Theilen wir nun das Intervall von 0 bis 1 in m gleiche Intervalle, welche durch die Werthe

$$\frac{0}{m}, \frac{1}{m}, \frac{2}{m} \cdots \frac{m-1}{m}, \frac{m}{m}$$

begrenzt werden, so muss, da die Anzahl $m+1$ der Zahlenpaare x, y grösser ist als die Anzahl m dieser Intervalle, wenigstens eines dieser Intervalle mehr als einen, also mindestens zwei von den Werthen $x - y\sqrt{D}$ enthalten, die zwei *verschiedenen* Werthen von y entsprechen. Wir bezeichnen diese beiden Werthe mit $x' - y'\sqrt{D}$ und $x'' - y''\sqrt{D}$; dann ist, abgesehen vom Vorzeichen, ihr Unterschied

$$(x' - x'') - (y' - y'')\sqrt{D} = x - y\sqrt{D} < \frac{1}{m},$$

und da y', y'' ungleich, nicht negativ und $\leqq m$ sind, so ist (abgesehen vom Vorzeichen) auch $y = y' - y'' \leqq m$ und von Null verschieden; mithin wird $x - y\sqrt{D}$ auch $< y^{-1}$ und von Null verschieden, weil $\sqrt{D}$ irrational ist. Hieraus folgt aber, wie oben, dass

$$x^2 - Dy^2 < 1 + 2\sqrt{D}$$

und von Null verschieden wird.

Dass nun aber auch unendlich viele solche Zahlenpaare x, y existiren, ergiebt sich leicht; sind nämlich schon beliebig viele solche Zahlenpaare x, y gefunden, so kann man immer die ganze Zahl m so gross nehmen, dass m^{-1} kleiner wird als der kleinste der bisher gefundenen Werthe $x - y\sqrt{D}$; für diese Zahl m erhält man aber auf die angegebene Weise wieder ein Zahlenpaar x, y von der Beschaffenheit, dass $x - y\sqrt{D} < m^{-1}$ und folglich auch kleiner als alle früher gefundenen Werthe $x - y\sqrt{D}$ wird, woraus folgt, dass dieses Zahlenpaar x, y von den frühern verschieden ist; mithin ist die Anzahl dieser Zahlenpaare unbegrenzt.

§. 142.

Mit Hülfe dieses Resultates, dass immer unendlich viele Paare von ganzen Zahlen x, y existiren, für welche der absolute Werth von $x^2 - Dy^2 < 1 + 2\sqrt{D}$ und von Null verschieden wird, lässt sich nun leicht beweisen, dass die Gleichung $t^2 - Du^2 = 1$ immer in ganzen Zahlen t, u lösbar ist, und zwar so, dass u von Null verschieden ausfällt.

Da die Anzahl der ganzen Zahlen, welche abgesehen vom Vorzeichen $< 1 + 2\sqrt{D}$ sind, endlich ist, so muss der Ausdruck $x^2 - Dy^2$ für unendlich viele Zahlenpaare x, y einer und derselben (von Null verschiedenen) Zahl k gleich werden; da ferner die Anzahl der verschiedenen Paare von Resten α, β, welche zwei Zahlen x, y (mod. k) lassen können, endlich, nämlich $= k^2$ ist, so leuchtet ebenso ein, dass mindestens ein solches Restsystem α, β unendlich oft auftreten muss, dass also unter den unendlich vielen Zahlenpaaren x, y, für welche $x^2 - Dy^2 = k$ wird, auch wieder unendlich viele Paare x, y sich finden müssen, in welchen $x \equiv \alpha$, $y \equiv \beta$ (mod. k) ist, wo α, β zwei bestimmte Reste bedeuten. Sind nun x', y' und x'', y'' irgend zwei solche Zahlenpaare, d. h. ist gleichzeitig

$$x'^2 - Dy'^2 = x''^2 - Dy''^2 = k$$

und

$$x' \equiv x'', \quad y' \equiv y'' \ (\text{mod. } k),$$

so kann man

$$(x' - y'\sqrt{D})(x'' + y''\sqrt{D}) = k(t + u\sqrt{D})$$

setzen, wo t, u *ganze* Zahlen bedeuten, die offenbar der Gleichung

$$t^2 - Du^2 = 1$$

genügen; und zwar dürfen wir annehmen, dass u von Null verschieden ist; denn aus $u = 0$, $t = \pm 1$ ergiebt sich vermöge der obigen Gleichung $x' - y'\sqrt{D} = \pm (x'' - y''\sqrt{D})$; da aber unendlich viele solche Zahlenpaare x', y' und x'', y'' existiren, so können wir auch immer zwei solche auswählen, dass x'', y'' verschieden von $\pm x'$, $\pm y'$, und folglich u von Null verschieden ausfällt.

Hiermit ist also in der That bewiesen, dass immer eine Lösung t, u der vorstehenden Pell'schen Gleichung existirt, in welcher u von Null verschieden ist.

Hieraus lässt sich dann (wie in §. 85), ebenfalls ohne Hülfe der Theorie der reducirten Formen, zeigen, dass alle Auflösungen t, u sich aus der Gleichung

$$t + u\sqrt{D} = \pm (T + U\sqrt{D})^n$$

ergeben, wo T, U die kleinsten positiven ganzen Zahlen bedeuten, die der Gleichung genügen, und der Exponent n alle positiven und

negativen ganzen Zahlen durchläuft. Nur in der einen Beziehung bleibt diese Theorie der Pell'schen Gleichung unvollständig, dass aus ihr keine directe Methode fliesst, diese kleinste positive Auflösung T, U unmittelbar zu finden. Hierzu und ebenso zur Beurtheilung der Aequivalenz zweier Formen und also auch der Darstellbarkeit einer Zahl durch eine Form bleibt die Theorie der reducirten Formen unentbehrlich.

IX. Ueber die Convergenz und Stetigkeit einiger unendlichen Reihen.

§. 143.

Die von *Abel**) herrührende Methode der theilweisen Summation, welche in §. 101 bei der Untersuchung der Convergenz und Stetigkeit einer unendlichen Reihe angewendet ist, findet gewissermassen ihre Erschöpfung bei dem Beweise des folgenden allgemeinen Satzes, in welchem aus gewissen, von einander unabhängigen Voraussetzungen über zwei Grössenreihen

$$a_1, a_2, a_3 \ldots \qquad \text{(a)}$$

$$b_1, b_2, b_3 \ldots \qquad \text{(b)}$$

Schlüsse auf die aus ihnen zusammengesetzte Grössenreihe

$$a_1 b_1, a_2 b_2, a_3 b_3 \ldots$$

gezogen werden.

Wenn bei unbegrenzt wachsendem n der Modulus der Summe

$$A_n = a_1 + a_2 + \cdots + a_n$$

endlich bleibt, wenn ferner die aus den Moduln der Differenzen $b_1 - b_2$, $b_2 - b_3$ ... gebildete Reihe $\mathfrak{B}$ convergirt, und ausserdem b_n mit wachsendem n unendlich klein wird; so convergirt die Reihe

$$\mathfrak{P} = a_1 b_1 + a_2 b_2 + a_3 b_3 + \cdots,$$

und ihr Werth ändert sich stetig mit den Grössen (b), *vorausgesetzt, dass auch $\mathfrak{B}$ sich stetig ändert.*

---

*) *Recherches sur la série etc.*, Œuvres complètes. 1839. T. I. p. 66; Crelle's Journal I. p. 311.

Aus der Annahme, dass der Modulus von A_n stets kleiner als eine angebbare Constante H bleibt, und dass die Reihe $\mathfrak{B}$ einen endlichen Werth besitzt, folgt zunächst die unbedingte Convergenz der Reihe

$$\mathfrak{Q} = A_1(b_1 - b_2) + A_2(b_2 - b_3) + \cdots,$$

weil selbst die Moduln ihrer Glieder eine convergente Reihe bilden, deren Summe $< H\mathfrak{B}$ ist. Bezeichnet man nun die Summen der ersten n Glieder der Reihen $\mathfrak{P}$, $\mathfrak{Q}$ resp. mit P_n, Q_n, so ist $P_n = Q_{n-1} + A_n b_n$, und da b_n mit wachsendem n unendlich klein wird, so convergirt auch die Reihe $\mathfrak{P}$, und ihr Werth ist gleich dem der Reihe $\mathfrak{Q}$.

Es genügt daher, den letzten Theil des Satzes für die Reihe $\mathfrak{Q}$ nachzuweisen. Setzt man nun $\mathfrak{Q} = Q_n + \mathfrak{Q}_n$ und $\mathfrak{B} = B_n + \mathfrak{B}_n$, wo B_n die Summe der ersten n Glieder der Reihe $\mathfrak{B}$ bedeutet, so ist der Modul von $\mathfrak{Q}_n < H\mathfrak{B}_n$; bezeichnet man ferner mit $\mathfrak{Q}'$, Q'_n, $\mathfrak{B}'$ ... diejenigen Werthe von $\mathfrak{Q}$, Q_n, $\mathfrak{B}$ ..., welche einem bestimmten System (b′) entsprechen, so wird, wenn die veränderlichen Grössen b_n sich den Grössen b'_n unbegrenzt und zwar der Art annähern, dass $\mathfrak{B}$ sich dem Werthe $\mathfrak{B}'$ nähert, auch $\mathfrak{B}_n$ sich dem Grenzwerthe $\mathfrak{B}'_n$ nähern. Nun kann man, wie klein auch eine gegebene positive Grösse δ sein mag, immer n so gross wählen, dass $H\mathfrak{B}'_n < \delta$ ist; mithin wird im Verlaufe der Annäherung auch $H\mathfrak{B}_n$, und folglich auch der Modul des Restes $\mathfrak{Q}_n$ definitiv $< \delta$ werden, während der erste Bestandtheil Q_n sich seinem Grenzwerthe Q'_n nähert; hieraus folgt, dass der Modul von $\mathfrak{Q} - \mathfrak{Q}'$ schliesslich unter 2δ herabsinkt, dass also $\mathfrak{Q}$ sich dem Grenzwerthe $\mathfrak{Q}'$ nähert, was zu beweisen war*).

Dem vorstehenden Beweise des obigen Satzes fügen wir noch folgende Bemerkungen hinzu. Die Convergenz der Reihe $\mathfrak{Q}$ folgt schon aus den beiden Annahmen, dass A_n endlich bleibt, und dass die Reihe $\mathfrak{B}$ convergirt; zufolge der letzteren muss b_n mit wachsendem n sich einem bestimmten Grenzwerthe $\mathfrak{b}$ nähern, weil ja die aus den Differenzen $b_1 - b_2$, $b_2 - b_3$ ... gebildete Reihe

$$(b_1 - b_2) + (b_2 - b_3) + \cdots = b_1 - \mathfrak{b}$$

*) Offenbar bleibt $\mathfrak{P} = \mathfrak{Q}$ auch dann noch stetig, wenn die oben als constant vorausgesetzten Grössen (a) sich zugleich der Art stetig ändern, dass das Maximum H der Moduln von A_n auch während der Aenderung endlich bleibt.

ebenfalls convergiren muss; aber dieser Grenzwerth $\mathfrak{b}$ kann sehr wohl von Null verschieden sein, und es leuchtet ein, dass in diesem Fall die Reihe $\mathfrak{P}$ stets und nur dann convergirt, wenn A_n mit wachsendem n sich ebenfalls einem bestimmten Grenzwerthe $\mathfrak{A}$ nähert, d. h. wenn die Reihe

$$\mathfrak{A} = a_1 + a_2 + a_3 + \cdots$$

convergirt; und zwar ist dann $\mathfrak{P} = \mathfrak{Q} + \mathfrak{A}\mathfrak{b}$. Durch diese Verschärfung der Annahme über die Constanten (a) wird es also gestattet, die Annahme $\mathfrak{b} = 0$ aufzugeben, während die Annahme, dass $\mathfrak{B}$ einen endlichen Werth besitzt, bestehen bleibt*). Von besonderer Wichtigkeit ist aber die Bemerkung, dass jetzt die Reihe $\mathfrak{P}$ sich schon dann mit den Grössen (b) *stetig* ändert, wenn $\mathfrak{B}$ im Verlaufe der Aenderung *endlich* bleibt, während $\mathfrak{Q}$ mit $\mathfrak{B}$ und $\mathfrak{b}$ auch *unstetig* werden kann. Setzt man nämlich $\mathfrak{A} = A_n + \mathfrak{A}_n$, so wird $a_n = \mathfrak{A}_{n-1} - \mathfrak{A}_n$, und

$$\mathfrak{P} = \mathfrak{A} b_1 - \mathfrak{A}_1 (b_1 - b_2) - \mathfrak{A}_2 (b_2 - b_3) - \cdots;$$

ist nun δ eine beliebig kleine positive gegebene Grösse, so kann man ν so gross wählen, dass für *alle***) Werthe $n \geqq \nu$ der Modul von $\mathfrak{A}_n < \delta$ wird; während daher die Summe der ersten ν Glieder rechter Hand sich stetig mit den Grössen (b) ändert, bleibt der Modul des Restes $< \delta\mathfrak{B}$ und kann folglich, da $\mathfrak{B}$ endlich bleibt, durch δ so klein gemacht werden, wie man will; mithin ändert sich $\mathfrak{P}$ stetig, was zu beweisen war.

---

*) Die Grössenreihen (b), denen endliche Werthe $\mathfrak{B}$ entsprechen, besitzen unter andern merkwürdigen Eigenschaften die, dass aus je zwei solchen Systemen (b′), (b″) unendlich viele andere abgeleitet werden können, deren allgemeines Glied $c + c' b'_n + c'' b''_n$ ist, wo c, c', c'' beliebige, von n unabhängige Grössen bedeuten.

**) Ist das System (a) ebenfalls veränderlich, so ist die Voraussetzung, dass $\mathfrak{A}$ sich stetig mit den Grössen (a) ändert, noch nicht hinreichend für die Stetigkeit von $\mathfrak{P}$, wovon man sich durch die genaue Prüfung des folgenden Beispiels überzeugen wird. Es sei $\psi(x)$ eine stetige Function, welche sowohl für unendlich kleine als auch für unendlich grosse Werthe x unendlich klein wird, wie z. B. $x:(1+x^2)$; ist nun $h \geqq 0$ eine veränderliche Grösse, und $a_n = \psi(nh) - \psi((n-1)h)$, ferner $b_n = 1 - nh$ oder $= 0$, je nachdem $nh < 1$ oder > 1 ist, so nähert sich $\mathfrak{P}$, wenn h unendlich klein wird, nicht dem Werthe Null, welcher $h = 0$ entspricht, sondern dem Werthe

$$\int_0^1 \psi(x)\, dx,$$

obgleich $\mathfrak{A}$ stetig $= 0$, und $\mathfrak{B}$ zwar nicht stetig, aber doch endlich bleibt.

Wir wollen die vorstehenden Principien auf die *Dirichlet'schen Reihen* anwenden; unter dieser Benennung verstehen wir Reihen von folgender Form*)

$$f(s) = \frac{a_1}{k_1^s} + \frac{a_2}{k_2^s} + \frac{a_3}{k_3^s} + \cdots,$$

wo $k_1, k_2\ k_3 \ldots$ positive Constanten von der Art bedeuten, dass $k_n \leqq k_{n+1}$ ist, und dass k_n mit n über alle Grenzen wächst; die Constanten $a_1, a_2, a_3 \ldots$ sind beliebige reelle oder complexe Grössen; ebenso kann die Veränderliche s beliebige reelle oder complexe Werthe annehmen, doch wollen wir uns hier der Einfachheit halber auf *reelle* Werthe s beschränken. Behält A_n die frühere Bedeutung, so ergiebt sich folgender Satz:

Bleibt A_n endlich bei wachsendem n, so convergirt die Reihe $f(s)$ für alle positiven Werthe s und ist nebst ihren sämmtlichen Derivirten stetig; convergirt die Reihe noch für $s = 0$, so ist sie auch an dieser Stelle stetig.

Die Behauptungen über $f(s)$ folgen unmittelbar aus der allgemeinen Untersuchung, wenn man $b_n = k_n^{-s}$ setzt, wodurch $\mathfrak{P}$ in die obige Reihe übergeht; denn $\mathfrak{B}$ ist $= k_1^{-s}$ oder $= 0$, je nachdem $s > 0$ oder $= 0$ ist. Um auch die Endlichkeit und Stetigkeit ihrer Derivirten $f'(s)$ darzuthun, setzen wir, wenn s einen festen positiven Werth, und ε eine sehr kleine positive oder negative Grösse bedeutet,

$$b_n = \frac{1}{\varepsilon}\left(\frac{1}{k_n^s} - \frac{1}{k_n^{s+\varepsilon}}\right),$$

so wird

$$\mathfrak{P} = \frac{f(s) - f(s+\varepsilon)}{\varepsilon}.$$

Wählt man nun ν so gross, dass $s \log k_\nu > 1$, und ε so klein, dass

$$\frac{s}{\varepsilon} \log\left(1 + \frac{\varepsilon}{s}\right) < s \log k_\nu$$

ist, so ist $b_\nu \geqq b_{\nu+1} \geqq b_{\nu+2} \ldots$, weil die Derivirte der Function

$$\frac{1}{\varepsilon}\left(\frac{1}{x^s} - \frac{1}{x^{s+\varepsilon}}\right)$$

*) Sie nehmen die Gestalt von Potenzenreihen an, wenn man $s = -\log x$ setzt.

für alle Werthe $x \geqq k_\nu$ negativ ist; ausserdem ist $\mathfrak{b} = 0$, also $\mathfrak{B}_{\nu-1} = b_\nu$. Wird nun ε unendlich klein, so nähert sich b_n dem Grenzwerthe

$$b'_n = \frac{\log k_n}{k_n^s},$$

und da $b'_\nu \geqq b'_{\nu+1} \geqq b'_{\nu+2} \ldots$, ferner $\mathfrak{b}' = 0$, also $\mathfrak{B}'_{\nu-1} = b'_\nu$ ist, so geht $\mathfrak{B}_{\nu-1}$ stetig in den Grenzwerth $\mathfrak{B}'_{\nu-1}$, und folglich auch $\mathfrak{B}$ stetig in den Werth $\mathfrak{B}'$ über. Mithin nähert sich auch $\mathfrak{P}$ dem Grenzwerthe $\mathfrak{P}'$, d. h. es ist

$$-f'(s) = \frac{a_1 \log k_1}{k_1^s} + \frac{a_2 \log k_2}{k_2^s} + \cdots,$$

und da diese Reihe wieder von derselben Beschaffenheit ist, so wird $f'(s)$ auch eine *stetige* Function von s. Ganz ähnlich lässt sich der Beweis für die Derivirten höherer Ordnung führen.

§. 144.

Der wahre Charakter des zuletzt bewiesenen Satzes besteht darin, dass aus dem Verhalten einer Dirichlet'schen Reihe $f(s)$ für $s = 0$ ein Schluss auf ihr Verhalten für alle positiven Werthe s gezogen wird (man kann ihn leicht so umformen, dass von dem beliebigen Werthe $s = \sigma$ auf alle Werthe $s > \sigma$ geschlossen wird). Unter diesem Gesichtspuncte erscheint von besonderm Interesse eine Vergleichung dieses Satzes mit dem allgemeinen Princip des §. 118; beachtet man nämlich, dass, wenn die dort mit t bezeichnete Grösse zwischen k_n und $k_{n+1} > k_n$ liegt, die entsprechende Grösse $T = n$ nichts Anderes ist, als die Summe der ersten n Glieder der Reihe

$$\frac{1}{k_1^{1+s}} + \frac{1}{k_2^{1+s}} + \frac{1}{k_3^{1+s}} + \cdots$$

für $s = -1$, so erkennt man, dass dort aus dem Verhalten der Reihe für $s = -1$ ein Schluss auf ihr Verhalten für alle positiven Werthe s, und namentlich auf ihr Verhalten an der Stelle $s = 0$ gezogen wird. Eine genauere, auf die Vereinigung und Verallgemeinerung beider Sätze hinzielende Untersuchung führt zu den nachstehenden Resultaten, in welchen zur Abkürzung

$$S_n = \frac{a_1}{k_1^s} + \frac{a_2}{k_2^s} + \cdots + \frac{a_n}{k_n^s}$$

gesetzt ist, während A_n seine frühere Bedeutung behält.

1. *Bleibt $S_n k_n^s$ für einen bestimmten negativen Werth s endlich bei wachsendem n, so gilt Dasselbe für jeden negativen Werth s, und ebenso bleibt $A_n : \log k_n$ endlich.*

2. *Bleibt $A_n : \log k_n$ endlich bei wachsendem n, so convergirt die Reihe $f(s)$ für jeden positiven Werth s.*

3. *Nähern sich $s\,S_n k_n^s$ und $s\,S_n k_{n+1}^s$ für einen bestimmten negativen Werth s bei wachsendem n einem gemeinschaftlichen Grenzwerthe $-\omega$, so gilt Dasselbe für jeden negativen Werth s, und ebenso nähern sich $A_n : \log k_n$ und $A_n : \log k_{n+1}$ dem gemeinschaftlichen Grenzwerthe $+\omega$.*

4. *Nähern sich $A_n : \log k_n$ und $A_n : \log k_{n+1}$ bei wachsendem n einem gemeinschaftlichen Grenzwerthe ω, so nähert sich $s f(s)$, wenn s positiv unendlich klein wird, demselben Grenzwerthe ω.*

Offenbar entspringt der Satz des vorigen Paragraphen aus 2., und der Satz des §. 118 aus 3. und 4.; um die Beweise kurz zu führen, bemerken wir, dass, wenn

$$R_n = \frac{a_1}{k_1^r} + \frac{a_2}{k_2^r} + \cdots + \frac{a_n}{k_n^r}$$

gesetzt wird,

$$S_n - R_n k_n^{r-s} = R_1 (k_1^{r-s} - k_2^{r-s}) + \cdots + R_{n-1} (k_{n-1}^{r-s} - k_n^{r-s})$$

ist; zerlegt man die Summe rechter Hand in zwei Bestandtheile, von denen der eine die ersten $(m-1)$ Glieder, der andere die übrigen $(n-m)$ Glieder enthält, und berücksichtigt, dass man allgemein

$$\frac{k_\nu^{r-s} - k_{\nu+1}^{r-s}}{r-s} = \int_{k_{\nu+1}}^{k_\nu} x^{r-s-1}\,dx = h_\nu^r \int_{k_{\nu+1}}^{k_\nu} x^{-s-1}\,dx = h_\nu^r\,\frac{k_{\nu+1}^{-s} - k_\nu^{-s}}{s}$$

setzen kann, wo $k_\nu \leqq h_\nu \leqq k_{\nu+1}$ ist, so erhält man

$$S_n - R_n k_n^{r-s} = \frac{r-s}{s}\left\{M(k_m^{-s} - k_1^{-s}) + N(k_n^{-s} - k_m^{-s})\right\},$$

wo M und N Mittelwerthe*) aus den Grössen $R_\nu h_\nu^r$ resp. von

*) Unter einem Mittelwerthe aus complexen Grössen z ist jeder complexe Werth ζ von der Beschaffenheit zu verstehen, dass die reellen Bestandtheile von ζ und ζi resp. Mittelwerthe aus den reellen Bestandtheilen der Grössen z und der Grössen zi sind.

$\nu = 1$ bis $\nu = m - 1$, und von $\nu = m$ bis $\nu = n - 1$ bedeuten. Nimmt man nun, wie im *dritten* Satze an, dass die Grössen $r R_\nu k_\nu^r$, $r R_\nu k_{\nu+1}^r$, also auch die Grössen $r R_\nu h_\nu^r$ mit wachsendem ν sich einem Grenzwerthe $-\omega$ nähern, und lässt man m mit n, doch so langsam über alle Grenzen wachsen, dass $k_m : k_n$ unendlich klein wird, so nähert sich rN dem Grenzwerthe $-\omega$, während M endlich bleibt, und folglich wird, wenn s negativ ist, $s S_n k_n^s$ sich ebenfalls dem Grenzwerthe $-\omega$ nähern. Ist aber $s = 0$, so folgt

$$A_n - R_n k_n^r = r\left\{M \log\left(\frac{k_1}{k_m}\right) + N \log\left(\frac{k_m}{k_n}\right)\right\},$$

und wenn man m der Art mit n über alle Grenzen wachsen lässt, dass $\log k_m : \log k_n$ unendlich klein wird, so ergiebt sich, dass $A_n : \log k_n$ sich dem Werthe $+\omega$ nähert. Die Behauptungen über $s S_n k_{n+1}^s$ und $A_n : \log k_{n+1}$ ergeben sich von selbst, weil aus der Annahme hervorgeht, dass, wenn ω von Null verschieden ist, nothwendig $k_n : k_{n+1}$ sich dem Werthe 1 nähert. Zugleich leuchtet ein, dass der Beweis des *ersten* Satzes auf dieselbe Weise geführt werden kann, und zwar viel einfacher, weil es gar keiner Zerlegung der obigen Summe in zwei Bestandtheile bedarf*).

Der Beweis des *zweiten* und *vierten* Satzes lässt sich in ähnlicher Weise führen; setzt man nämlich, wenn s einen *positiven* Werth hat,

$$K_n = \int_{k_n}^{\infty} \frac{s \log x\, dx}{x^{s+1}} = \frac{1 + s \log k_n}{s k_n^s},$$

so ist

$$K_n - K_{n+1} = \int_{k_n}^{k_{n+1}} \frac{s \log x\, dx}{x^{s+1}} = \log h_n (k_n^{-s} - k_{n+1}^{-s});$$

nimmt man daher an, dass $A_n : \log k_n$ endlich bleibt, so folgt hieraus leicht**), dass die unendliche Reihe

---

*) Die auf den ersten Blick auffallende Erscheinung, dass der obige Beweis auch für positive Werthe r gilt, hängt mit ähnlichen Sätzen über das Verschwinden von $f(s) - S_n$ für positive Werthe s bei wachsendem n zusammen.

**) Offenbar darf man, ohne die Allgemeinheit der Sätze zu beeinträchtigen, bei ihrem Beweise annehmen, dass schon $k_1 > 1$ ist.

$$A_1(k_1^{-s} - k_2^{-s}) + A_2(k_2^{-s} - k_3^{-s}) + \cdots$$
$$= \frac{A_1}{\log h_1}(K_1 - K_2) + \frac{A_2}{\log h_2}(K_2 - K_3) + \cdots$$

convergirt, und dass ihre Summe mit $f(s)$ übereinstimmt, womit der zweite Satz bewiesen ist. Bezeichnet man ferner mit M und M' Mittelwerthe aus den Grössen $A_n : \log h_n$ resp. von $n = 1$ bis $n = m - 1$, und von $n = m$ bis $n = \infty$, so kann man

$$f(s) = M(K_1 - K_m) + M' K_m$$

setzen; nimmt man nun (wie im vierten Satze) an, dass die Grössen $A_n : \log k_n$ und $A_n : \log k_{n+1}$ sich einem gemeinschaftlichen Grenzwerthe ω nähern, so gilt Dasselbe von $A_n : \log h_n$; lässt man daher, während s positiv unendlich klein wird, gleichzeitig m über alle Grenzen, doch so langsam wachsen, dass $s \log k_m$ unendlich klein wird, so nähert sich M' dem Grenzwerthe ω, während M endlich bleibt, und da sK_1 und sK_m sich dem gemeinschaftlichen Grenzwerthe 1 nähern, so nähert sich $sf(s)$ dem Grenzwerthe ω, was zu beweisen war.

Nachdem die obigen Sätze bewiesen sind, führen wir einige Beispiele an, hauptsächlich um zu zeigen, dass sie nicht ohne Weiteres umgekehrt werden dürfen.

Beispiel 1. Ist $c > 1$, und $s > 0$, so ist

$$f(s) = \frac{a}{c^s} + \frac{b}{c^{2s}} + \frac{a}{c^{3s}} + \frac{b}{c^{4s}} + \cdots = \frac{ac^s + b}{c^{2s} - 1};$$

für jeden negativen Werth s ist bei wachsendem n

$$\lim S_{2n} c^{2ns} = \frac{ac^s + b}{1 - c^{2s}}, \quad \lim S_{2n+1} c^{(2n+1)s} = \frac{a + bc^s}{1 - c^{2s}},$$

also schwankt $S_n k_n^s$, und nur, wenn $b = a$ ist, wird

$$\lim S_n k_n^s = \frac{a}{1 - c^s};$$

trotzdem ist, auch wenn a und b ungleich sind,

$$\lim \frac{A_n}{\log k_n} = \lim \frac{A_n}{\log k_{n+1}} = \frac{a + b}{2 \log c},$$

und wirklich nähert sich $sf(s)$ für unendlich kleine positive Werthe von s demselben Grenzwerth.

Beispiel 2. Ist wieder $c > 1$, und $s > 0$, so ist

$$f(s) = \frac{1}{c^s} - \frac{2}{c^{2s}} + \frac{3}{c^{3s}} - \frac{4}{c^{4s}} + \cdots = \frac{c^s}{(c^s+1)^2};$$

da $A_{2n} = -n$, $A_{2n-1} = +n$ ist, so schwankt $A_n : \log k_n$; dennoch nähert sich $sf(s)$ dem bestimmten Grenzwerth Null, wenn s positiv unendlich klein wird.

Beispiel 3. Von grösserem Interesse ist die folgende Reihe

$$f(s) = e^{-s} + ce^{-sc} + c^2 e^{-sc^2} + c^3 e^{-sc^3} + \cdots,$$

wo c wieder > 1 ist; da $\log k_n = c^{n-1}$, und

$$A_n = 1 + c + c^2 + \cdots + c^{n-1} = \frac{c^n - 1}{c-1},$$

so ergiebt sich bei wachsendem n

$$\lim \frac{A_n}{\log k_n} = \frac{c}{c-1}, \quad \lim \frac{A_n}{\log k_{n+1}} = \frac{1}{c-1},$$

und es zeigt sich, dass $sf(s)$ für unendlich kleine positive Werthe von s sich keinem Grenzwerthe nähert, sondern hin- und herschwankt. Ist nämlich r ein bestimmter positiver Werth, und lässt man $s = rc^{-\varrho}$ dadurch unendlich klein werden, dass ϱ wachsend alle positiven ganzen Zahlen durchläuft, so nähert sich $sf(s)$ dem bestimmten, aber von r abhängigen Grenzwerth

$$\psi(r) = \Sigma\, rc^n e^{-rc^n},$$

wo n alle ganzen Zahlen von $-\infty$ bis $+\infty$ durchlaufen muss. Offenbar ist $\psi(r)$ eine periodische Function von $\log r$, welche sich in die Fourier'sche Reihe

$$\frac{1}{\log c}\, \Sigma\, z^n\, \Pi\left(\frac{2n\pi i}{\log c}\right)$$

verwandeln lässt, wo $\log z \log c = -2\pi i \log r$ ist, Π das Euler'sche Integral zweiter Art bedeutet, und n alle ganzen Zahlen von $-\infty$ bis $+\infty$ durchläuft; sie convergirt für jeden complexen Werth r, dessen reeller Bestandtheil positiv ist; sie ist zugleich der Grenzwerth des Integrals

$$\int_{-\infty}^{+\infty} rc^x e^{-rc^x} dx . \frac{\sin(2n+1)\pi x}{\sin \pi x}$$

für unendlich grosse Werthe der positiven ganzen Zahl n. Wird s stetig positiv unendlich klein, so schwankt $sf(s)$ um den mittlern Werth $1 : \log c$, welcher auch zwischen den Grenzwerthen von $A_n : \log k_n$ und $A_n : \log k_{n+1}$ liegt.

X. Ueber die Composition der binären quadratischen Formen.

§. 145.

Den Ausgangspunct für unsere Darstellung der von *Gauss**) gegründeten Theorie der Composition bildet folgendes Lemma:

Ist

$$bb \equiv D \ (mod.\ a), \quad b'b' \equiv D \ (mod.\ a'), \qquad (1)$$

und haben die drei Zahlen $a, a', b+b'$ *keinen gemeinschaftlichen Theiler, so existirt in Bezug auf den Modulus* aa' *eine und nur eine Classe von Zahlen* B, *welche den drei Bedingungen*

$$B \equiv b \ (mod.\ a), \quad B \equiv b' \ (mod.\ a'), \quad BB \equiv D \ (mod.\ aa') \qquad (2)$$

genügen.

Dies leuchtet unmittelbar ein, falls a und a' relative Primzahlen sind (§§. 25, 37); unter der allgemeineren Voraussetzung aber, dass $a, a', b+b'$ keinen gemeinschaftlichen Theiler haben, bestimme man (nach §. 24) drei ganze Zahlen h, h', h'', welche die Bedingung

$$ha + h'a' + h''(b+b') = 1 \qquad (3)$$

befriedigen; dann werden alle durch die Congruenz

$$B \equiv hab' + h'a'b + h''(bb' + D) \ (\text{mod. } aa') \qquad (4)$$

bestimmten Zahlen B und nur diese den Forderungen (2) genügen. Da nämlich

*) *D. A.* art. 234 seqq. — Vergl. *Lejeune Dirichlet: De formarum binariarum secundi gradus compositione.* 1851.

$$(B-b)(B-b') = BB-(b+b')B+bb'$$

ist, so folgt zunächst, dass die Forderungen (2) vollständig übereinstimmen mit den folgenden

$$a'B \equiv a'b,\ aB \equiv ab',\ (b+b')B \equiv bb'+D \pmod{aa'}, \quad (5)$$

welche, mit h', h, h'' multiplicirt und addirt, die Congruenz (4) nach sich ziehen. Dass umgekehrt jede durch die Congruenz (4) bestimmte Zahl B den Bedingungen (2) oder (5) genügt, ergiebt sich leicht, wenn man aus (3) und (4) der Reihe nach h', h, h'' eliminirt und hierbei die Voraussetzungen (1) berücksichtigt.

Wir bemerken schliesslich, dass die Zahlen a, a', $2B$ keinen gemeinschaftlichen Theiler haben; denn ist δ ein solcher, so folgt aus (2) auch $b \equiv b' \equiv B \pmod{\delta}$, also $b + b' \equiv 2B \equiv 0 \pmod{\delta}$; mithin ist δ gemeinschaftlicher Theiler von a, a', $b + b'$, und folglich $\delta = 1$.

§. 146.

Zwei binäre quadratische Formen (a, b, c), (a', b', c') von gleicher Determinante D sollen *einig**) heissen, wenn die Zahlen a, a', $b+b'$ keinen gemeinschaftlichen Theiler haben. Da unter dieser Voraussetzung auch $bb \equiv D \pmod{a}$, $b'b' \equiv D \pmod{a'}$ ist, so folgt aus dem vorhergehenden Lemma unmittelbar die Existenz von unendlich vielen (nach §. 56 äquivalenten) Formen (aa', B, C) derselben Determinante D, deren mittlere Coefficienten B den Bedingungen $B \equiv b \pmod{a}$, $B \equiv b' \pmod{a'}$ genügen; jede solche Form (aa', B, C) heisse *zusammengesetzt***) *(composita) aus* (a,b,c) *und* (a', b', c').

Wir bemerken zunächst, dass (nach §. 56) die Formen (a, b, c), (a', b', c') resp. den Formen $(a, B, a'C)$, (a', B, aC) äquivalent sind; diese letzteren sind ebenfalls einig, weil die Zahlen a, a', $2B$, keinen gemeinschaftlichen Theiler haben (§. 145), und aus ihnen ist ebenfalls die Form (aa', B, C) zusammengesetzt. Bedeuten nun x, y, x', y' variabele Grössen, und setzt man

---

*) Diese Benennung soll an die *radices concordantes* von *Dirichlet* erinnern.

**) Vergl. *Gauss*: *D. A.* artt. 235, 242, 243, 244.

$$X = xx' - Cyy', \quad Y = (ax + By)\,y' + (a'x' + By')y, \quad (1)$$

so wird

$$(ax + (B + \sqrt{D})y)(a'x' + (B + \sqrt{D})y') = aa'X + (B + \sqrt{D})\,Y; \quad (2)$$

ersetzt man hierin $\sqrt{D}$ durch $-\sqrt{D}$ und multiplicirt die so entstehende Gleichung mit der vorstehenden, so ergiebt sich nach Wegwerfung des beiden Seiten gemeinschaftlichen Factors aa' die Gleichung

$$\begin{aligned}(ax^2 + 2Bxy + a'Cy^2)\,(a'x'^2 + 2Bx'y' + aCy'^2) \\ = aa'X^2 + 2BXY + CY^2,\end{aligned} \quad (3)$$

d. h. *die Form* (aa', B, C) *geht durch die bilineare Substitution* (1) *in das Product aus den beiden Formen* $(a, B, a'C)$, (a', B, aC) *über.*

Auf dem vorstehenden Resultate beruht zugleich der Beweis des folgenden Fundamentalsatzes*):

Sind die beiden einigen Formen (a, b, c), (a', b', c') *resp. äquivalent den beiden einigen Formen* (m, n, l), (m', n', l'), *so ist auch die aus den beiden ersteren zusammengesetzte Form* (aa', B, C) *äquivalent der aus den beiden letzteren zusammengesetzten Form* (mm', N, L).

Aus den Voraussetzungen folgt zunächst, dass die Formen $(a, B, a'C)$, (a', B, aC) resp. den Formen $(m, N, m'L)$, (m', N, mL) äquivalent sind, und hieraus (nach §. 60. Anmerkung) die Existenz von vier ganzen Zahlen x, y, x', y', welche den folgenden Bedingungen genügen

$$ax^2 + 2Bxy + a'Cy^2 = m,\ a'x'^2 + 2Bx'y' + aCy'^2 = m' \quad (4)$$

$$ax + (B + N)y \equiv 0,\ (B - N)x + a'Cy \equiv 0 \pmod{m} \quad (5)$$

$$a'x' + (B + N)y' \equiv 0,\ (B - N)x' + aCy' \equiv 0 \pmod{m'}, \quad (6)$$

und ebenso braucht man, um die Aequivalenz der beiden Formen (aa', B, C), (mm', N, L) darzuthun, nur die Existenz von zwei ganzen Zahlen X, Y nachzuweisen, welche die Forderungen

$$aa'X^2 + 2BXY + CY^2 = mm' \quad (7)$$

$$aa'X + (B + N)\,Y \equiv 0 \pmod{mm'} \quad (8)$$

$$(B - N)\ X + CY \equiv 0 \pmod{mm'} \quad (9)$$

befriedigen. Es lässt sich nun leicht zeigen, dass die beiden (offenbar ganzen) Zahlen X, Y, welche nach (1) aus den vier ganzen

*) *Gauss: D. A.* art. 239. — *Dirichlet* a. a. O.

Zahlen x, y, x', y' gebildet sind, in der That den vorstehenden Bedingungen genügen. Zunächst folgt (7) unmittelbar aus (3) und (4). Da ferner aus jeder Gleichung von der Form

$$(t+u\sqrt{D})\,(t'+u'\sqrt{D}) = (t''+u''\sqrt{D})\,(t'''+u'''\sqrt{D}),$$

wo t, u, t' u. s. w. ganze Zahlen bedeuten, die in Bezug auf die Variabele z identische Gleichung

$$(t+uz)\,(t'+u'z) = (t''+u''z)\,(t'''+u'''z) + (uu'-u''u''')\,(zz-D),$$

und hieraus, da $NN \equiv D$ (mod. mm') ist, auch die Congruenz

$$(t+uN)\,(t'+u'N) \equiv (t''+u''N)\,(t'''+u'''N) \pmod{mm'}$$

hervorgeht, so folgt (8) unmittelbar aus (2) unter Berücksichtigung von (5) und (6). Dieselbe Gleichung (2) lässt sich endlich durch Multiplication mit $B-\sqrt{D}$, oder mit C, und durch Division mit a oder mit a' auf die folgenden vier Formen bringen

$$((B-\sqrt{D})x+a'Cy)\,(a'x'+(B+\sqrt{D})y') = a'U$$
$$(ax+(B+\sqrt{D})y)\,((B-\sqrt{D})x'+aCy') = aU$$
$$((B-\sqrt{D})x+a'Cy)\,((B-\sqrt{D})x'+aCy') = (B-\sqrt{D})\,U$$
$$C(ax+(B+\sqrt{D})y)\,(a'x'+(B+\sqrt{D})y') = (B+\sqrt{D})\,U,$$

wo zur Abkürzung

$$(B-\sqrt{D})\,X+CY = U$$

gesetzt ist; ersetzt man überall $\sqrt{D}$ durch N, so gehen nach dem oben angeführten Princip diese Gleichungen wieder in Congruenzen nach dem Modulus mm' über; bezeichnet man den aus U hervorgehenden Ausdruck, d. h. die linke Seite der zu beweisenden Congruenz (9), mit V, so ergiebt sich unter Berücksichtigung von (5) und (6), dass die Producte $a'V$, aV, $(B-N)\,V$, $(B+N)\,V$, mithin auch $2BV$ durch mm' theilbar sind; da aber die Factoren a, a', $2B$ keinen gemeinschaftlichen Theiler haben, so muss der andere Factor V für sich allein durch mm' theilbar sein, also die Congruenz (9) wirklich Statt finden.

Mithin genügen die beiden ganzen Zahlen X, Y den Bedingungen (7), (8), (9), und hieraus folgt (nach §. 60. Anmerkung) die Aequivalenz der Formen (aa', B, C), (mm', N, L); was zu beweisen war.

§. 147.

Um den Charakter des eben bewiesenen Fundamentalsatzes in das rechte Licht zu setzen, bemerken wir zunächst Folgendes: *Sind* (a, b, c), (a', b', c') *zwei einige Formen, so sind ihre Theiler* σ, σ' (§. 61) *relative Primzahlen, und* $\sigma\sigma'$ *ist der Theiler der aus ihnen zusammengesetzten Form* $(aa'\ B,\ C)$. Denn da die Formen (a, b, c), (a', b', c') resp. den Formen $(a, B, a'C)$, (a', B, aC) äquivalent sind, so ist (nach §. 61) σ der grösste gemeinschaftliche Divisor von a, $2B$, $a'C$, und σ' ist der grösste gemeinschaftliche Divisor von a', $2B$, aC; da nun a, a', $2B$ keinen gemeinschaftlichen Divisor haben, so muss die in a und $2B$ aufgehende Zahl σ relative Primzahl zu a' (und also auch zu der in a' aufgehenden Zahl σ') sein; und da σ in $a'C$ aufgeht, so muss σ auch in C aufgehen; ebenso muss σ' relative Primzahl zu a sein und folglich auch in C aufgehen. Da ferner schon gezeigt ist, dass σ und σ' relative Primzahlen sind, und da beide sowohl in $2B$, als auch in C aufgehen, so ist $\sigma\sigma'$ offenbar gemeinschaftlicher Divisor der drei Zahlen aa', $2B$, C. Wollte man nun annehmen, $\sigma\sigma'$ wäre nicht ihr grösster gemeinschaftlicher Divisor, sondern sie liessen sich nach der Division mit $\sigma\sigma'$ noch durch eine Primzahl p theilen, so müsste p wenigstens in einer der beiden Zahlen $a:\sigma$ oder $a':\sigma'$ aufgehen; gesetzt aber, p ginge in $a:\sigma$ auf, so hätten die drei Zahlen a, $2B$, $a'C$ den gemeinschaftlichen Divisor $p\sigma$, während doch σ ihr grösster gemeinschaftlicher Divisor ist. Ebenso wenig kann p in $a':\sigma'$ aufgehen, und folglich ist $\sigma\sigma'$ der grösste gemeinschaftliche Divisor der Zahlen aa', $2B$, C, d. h. $\sigma\sigma'$ ist der Theiler der Form (aa', B, C), was zu beweisen war.

Umgekehrt: *hat man zwei Formenclassen* K, K' *von gleicher Determinante* D, *deren Theiler* σ, σ' *relative Primzahlen sind, so kann man stets zwei einige Formen* (a, b, c), (a', b', c') *resp. aus den Classen* K, K' *auswählen.* Denn man kann (nach §. 93) den Repräsentanten (a, b, c) der Classe K zunächst so wählen, dass a relative Primzahl zu σ' wird, worauf der Repräsentant (a', b', c') der Classe K' so gewählt werden kann, dass a' relative Primzahl zu a wird; dann sind aber (a, b, c), (a', b', c') gewiss zwei einige Formen. Wie nun auch zwei einige Formen aus den Classen K, K'

ausgewählt sein mögen, so wird zufolge des bewiesenen Fundamentalsatzes die aus ihnen zusammengesetzte Form stets einer und derselben Formenclasse $\mathfrak{K}$ von derselben Determinante D angehören, deren Theiler nach dem Obigen $= \sigma\sigma'$ ist. Wir werden daher sagen, dass diese *Classe* $\mathfrak{K}$ *aus den beiden einigen Classen* K, K' *zusammengesetzt* ist, und werden dies durch die symbolische Gleichung*)

$$\mathfrak{K} = KK' = K'K$$

ausdrücken.

Sind ferner je zwei der drei Classen K, K', K'' einig, so lassen sie sich successive zu einer Classe zusammensetzen, und zwar wird diese resultirende Classe von der Anordnung der beiden successiven Compositionen völlig unabhängig sein**); d. h. symbolisch ausgegedrückt, es wird

$$(KK')K'' = (KK'')K' = (K'K'')K$$

sein. Man kann nämlich die Repräsentanten (a, b, c), (a', b', c'), (a'', b'', c'') der drei Classen K, K', K'' (nach §. 93) so wählen, dass a, a', a'' relative Primzahlen sind; bestimmt man nun (nach §. 25) B durch die Congruenzen

$$B \equiv b \pmod{a},\ B \equiv b' \pmod{a'},\ B \equiv b'' \pmod{a''},$$

so wird von selbst $BB \equiv D \pmod{aa'a''}$, also $D = BB - aa'a''C$, wo C eine ganze Zahl bedeutet. Dann enthält

die Classe		K	die Form		$(a, B, a'a''C)$
„	„	K'	„	„	$(a', B, aa''C)$
„	„	K''	„	„	$(a'', B, aa'C)$
„	„	KK'	„	„	$(aa', B, a''C)$
„	„	KK''	„	„	$(aa'', B, a'C)$
„	„	$K'K''$	„	„	$(a'a'', B, aC)$

und jede der Classen $(KK')K''$, $(KK'')K'$, $(K'K'')K$ enthält folglich dieselbe Form $(aa'a'', B, C)$; mithin sind diese drei Classen identisch. Diese eine Classe kann daher einfach durch das Symbol $KK'K''$ bezeichnet werden, wobei die Stellung der drei Symbole K, K', K'' gleichgültig ist.

Wendet man nun dieselbe Schlussfolgerung an, wie in §. 2, so ergiebt sich, dass auch für jede grössere Anzahl von Classen

*) *Gauss* bezeichnet die aus K und K' zusammengesetzte Classe mit $K + K'$ (*D. A.* art. 249).

**) *Gauss: D. A.* artt. 240, 241.

$K, K' \ldots$ die durch ihre successive Composition entstehende Classe völlig bestimmt, und von der Anordnung der Composition gänzlich unabhängig ist. Erforderlich bleibt aber die Bedingung, dass diese Classen $K, K' \ldots$ zu derselben Determinante gehören, und dass ihre Theiler $\sigma, \sigma' \ldots$ relative Primzahlen sind, weil nur dann die Composition in der oben angegebenen Art ausgeführt werden kann; für unsere Zwecke reicht aber dieser specielle Fall der allgemeineren Theorie der Composition völlig aus.

§. 148.

Wir betrachten zunächst einige besonders wichtige specielle Fälle der Classencomposition *).

1. Die Hauptform $(1, 0, -D)$ ist offenbar einig mit jeder Form (a, b, c) derselben Determinante, und die Composition beider Formen giebt als Resultat dieselbe Form (a, b, c), also: *Durch Composition irgend einer Classe K mit der Hauptclasse entsteht immer die Classe K.* Bezeichnet man daher die Hauptclasse durch das Symbol 1, so ist immer $1K = K$, wo K eine beliebige Classe bedeutet.

2. Ist (a, b, c) eine ursprüngliche Form der ersten Art, so ist sie einig mit der Form (c, b, a), und aus beiden ist die Form $(ac, b, 1)$ zusammengesetzt. Da nun (c, b, a) mit $(a, -b, c)$, und ebenso $(ac, b, 1)$ mit $(1, -b, ac)$ und folglich auch mit der Hauptform $(1, 0, -D)$ äquivalent ist (§. 56), so kann man dies Resultat kurz so aussprechen: *Die Composition von zwei entgegengesetzten ursprünglichen Classen der ersten Art H, H' giebt stets die Hauptclasse* $HH' = 1$.

Hieraus ziehen wir eine wichtige Folgerung, von welcher sehr häufig Gebrauch gemacht wird: *Bedeutet H eine ursprüngliche Classe erster Art, so folgt aus* $HK = HL$ *auch stets* $K = L$. Ist nämlich H' der Classe H entgegengesetzt, also $HH' = 1$, so folgt aus $HK = HL$ zunächst $(HK)H' = (HL)H'$, und hieraus $(HH')K = (HH')L$, also $K = L$.

*) *Gauss: D. A.* artt. 243, 250.

3. Ist K eine Classe vom Theiler σ, so kann man (nach §. 93) ihren Repräsentanten $(a\sigma, b, c)$ so wählen, dass a relative Primzahl zu σ ist; dann ist diese Form offenbar zusammengesetzt aus den beiden einigen Formen $(a, b, c\sigma)$ und (σ, b, ac), deren letztere den Theiler σ hat und der einfachsten Classe dieses Theilers angehört (§. 61), woraus von selbst folgt, dass die erstere Form eine ursprüngliche Form der ersten Art sein muss, was sich auch leicht direct nachweisen liesse. Wir haben daher das Resultat: *Ist S die einfachste, und K irgend eine Classe vom Theiler σ, so giebt es immer mindestens eine ursprüngliche Classe erster Art H von der Beschaffenheit, dass $SH = K$ ist.*

Man überzeugt sich leicht mit Hülfe von 2., dass der Satz 3. auch dann noch gilt, wenn S und K irgend welche Classen desselben Theilers bedeuten; ebenso leuchtet ein, dass aus den einfachsten Classen der Theiler σ, σ' stets die einfachste Classe des Theilers $\sigma\sigma'$ zusammengesetzt ist, natürlich unter der Voraussetzung, dass σ und σ' relative Primzahlen sind. Wir verweilen aber nicht länger bei diesen und anderen ebenso leicht zu beweisenden Sätzen, weil sie für die nachfolgenden Untersuchungen völlig entbehrlich sind.

§. 149.

Durch Composition einer *ursprünglichen Classe der ersten Art A* mit sich selbst, oder kürzer, durch *Duplication**) der Classe A entsteht eine Classe AA, welche man auch durch A^2 bezeichnen kann; ähnlich ist die allgemeine Bezeichnung A^m zu verstehen, wo m irgend eine positive ganze Zahl bedeutet. Durch Anwendung derselben Schlüsse, wie in §. 28, findet man nun leicht, dass immer ein kleinster positiver Exponent δ existirt, welcher der Bedingung $A^\delta = 1$ genügt; dann sind die Classen

$$1, A, A^2 \ldots A^{\delta-1},$$

welche die sogenannte *Periode***) der Classe A bilden, von einander verschieden; aus $A^r = A^s$ folgt $r \equiv s \pmod{\delta}$, und umgekehrt; verallgemeinert man hiernach die Bezeichnung A^m, in-

*) *Gauss: D. A.* art. 249.

**) *Gauss: D. A.* art. 306. II.

dem man sie auch auf negative Exponenten m (und auf $m = 0$) ausdehnt, so ist z. B. $A^{-1} = A^{\delta-1}$ das Symbol für die Classe, welche der Classe A entgegengesetzt ist (§. 148, 2.).

Eine solche Classenperiode bildet nur einen speciellen Fall des folgenden neuen Begriffs, welcher von der höchsten Wichtigkeit für die Gesetze der Composition ist: Ein System $\mathfrak{A}$ von ursprünglichen Classen der ersten Art soll eine *Gruppe**) heissen, wenn die Composition von je zwei Classen des Systems $\mathfrak{A}$ immer wieder eine Classe desselben Systems liefert; die Anzahl a der in $\mathfrak{A}$ enthaltenen verschiedenen Classen heisse der *Grad* dieser Gruppe $\mathfrak{A}$.

Aus dieser Erklärung folgt sofort, dass, wenn die Classe A in einer Gruppe $\mathfrak{A}$ enthalten ist, auch die ganze Periode der Classe A, also auch die entgegengesetzte Classe A^{-1} und die Hauptclasse sich in $\mathfrak{A}$ vorfindet. Setzt man ferner jede in der Gruppe $\mathfrak{A}$ enthaltene Classe A_1, $A_2 \ldots A_a$ mit einer ursprünglichen Classe erster Art B zusammen, so sind die entstehenden Classen $A_1 B$, $A_2 B \ldots A_a B$ von einander verschieden (§. 148, 2.) und bilden einen Complex, den wir kurz durch $\mathfrak{A}B$ bezeichnen können; zwei so gebildete Complexe $\mathfrak{A}B$ und $\mathfrak{A}B'$ sind nun entweder vollständig identisch (was wieder durch das Zeichen $=$ angedeutet werden soll), oder sie haben keine einzige gemeinschaftliche Classe; denn wenn sie eine gemeinschaftliche Classe $AB = A'B'$ haben, wo A und A' in $\mathfrak{A}$ enthalten sind, so folgt $B = A^{-1} A' B' = A'' B'$, wo $A'' = A^{-1} A'$ eine ebenfalls in $\mathfrak{A}$ enthaltene Classe bedeutet, und hieraus $\mathfrak{A}B = \mathfrak{A}A''B'$ $= \mathfrak{A}B'$, weil offenbar der Complex $\mathfrak{A}A''$ mit $\mathfrak{A}$ selbst identisch ist.

Stützt man sich auf diese fundamentale Eigenschaft einer Gruppe und wendet dieselbe Schlussfolgerung an, wie in §. 127, so ergiebt sich unmittelbar folgender Satz:

Sind alle a Classen einer Gruppe $\mathfrak{A}$ zugleich in einer Gruppe $\mathfrak{B}$ vom Grade b enthalten, so ist a ein Divisor von $b = \mu a$, und die Gruppe $\mathfrak{B}$ besteht aus μ Complexen von der Form $\mathfrak{A}B$; die Gruppe $\mathfrak{A}$ soll daher auch ein *Divisor* der Gruppe $\mathfrak{B}$, letztere ein *Multiplum* der ersteren heissen.

*) Ich wähle absichtlich diese von *Galois* in die Algebra eingeführte Benennung, weil seine Theorie und die obige, welche den sogenannten Abel'schen Gleichungen entspricht, gemeinschaftlich enthalten sind in der allgemeineren Theorie der Composition, in welcher $(KK')K'' = K(K'K'')$ ist, und ausserdem sowohl aus $KK' = KK''$, als auch aus $K'K = K''K$ stets $K' = K''$ folgt (vergl. §. 55).

Sind ferner $\mathfrak{A}$ und $\mathfrak{B}$ zwei beliebige Gruppen, so bildet das System $\mathfrak{D}$ aller in $\mathfrak{A}$ und $\mathfrak{B}$ gemeinschaftlich enthaltenen Classen ebenfalls eine Gruppe, welche der grösste gemeinschaftliche Divisor von $\mathfrak{A}$ und $\mathfrak{B}$ heissen mag; sind a, b, d die Grade dieser drei Gruppen, so ist d ein gemeinschaftlicher Divisor von $a = \alpha d$ und $b = \beta d$; besteht ferner die Gruppe $\mathfrak{B}$ aus den β Complexen $\mathfrak{D} B_1$, $\mathfrak{D} B_2 \ldots \mathfrak{D} B_\beta$, so bilden, wie man leicht erkennt, auch die β Complexe $\mathfrak{A} B_1$, $\mathfrak{A} B_2 \ldots \mathfrak{A} B_\beta$ eine Gruppe $\mathfrak{M}$ vom Grade $m = a\beta = b\alpha = ab:d$, und zwar ist diese Gruppe $\mathfrak{M}$ das kleinste gemeinschaftliche Multiplum der beiden Gruppen $\mathfrak{A}$ und $\mathfrak{B}$*).

Die am leichtesten zu überblickenden Gruppen sind die oben erwähnten Perioden; jede solche Gruppe, deren Classen durch wiederholte Composition aus einer einzigen Classe entstehen, wollen wir eine *reguläre* Gruppe nennen; jede *irrreguläre* Gruppe lässt sich als das kleinste Multiplum von gewissen regulären Gruppen darstellen, von denen je zwei nur die Hauptclasse gemeinschaftlich haben. Auf diese Darstellung und die damit zusammenhängenden Sätze von *Gauss***), deren Beweis leicht auf das Vorhergehende gegründet werden kann, wollen wir aber hier nicht mehr eingehen.

§. 150.

Eine der hauptsächlichsten Anwendungen, welche *Gauss* von der Theorie der Composition gemacht hat, besteht in der Vergleichung der Anzahl h' der Classen vom Theiler σ mit der Anzahl h der ursprünglichen Classen erster Art***); offenbar ist dies dieselbe Aufgabe, welche Dirichlet in der oben mitgetheilten Art (§§. 97, 99, 100) gelöst hat.

Bedeutet S die einfachste, und K irgend eine Classe vom Theiler σ, so existirt (nach §. 148, 3.) *mindestens* eine ursprüngliche Classe erster Art H, welche mit S componirt die Classe K

*) Dieser Satz verliert seine allgemeine Gültigkeit, wenn die *Ordnung* der zusammenzusetzenden Elemente einen Einfluss auf das Compositum hat.

**) *D. A.* artt. 305—307; ferner *Démonstration de quelques théorèmes concernants les périodes des classes des formes binaires du second degré* (Gauss Werke, Bd. II. p. 266. 1863). — Vergl. *Schering: Die Fundamental-Classen der zusammensetzbaren arithmetischen Formen.* Göttingen 1869.

***) *D. A.* artt. 253—256.

hervorbringt; durch Composition von S mit allen h Classen H müssen also jedenfalls alle Classen K vom Theiler σ, jede mindestens einmal erzeugt werden. Es seien nun $R_1, R_2 \ldots R_r$ die sämmtlichen r von einander verschiedenen ursprünglichen Classen erster Art, welche mit S componirt die Classe S selbst hervorbringen; da aus $SR = S$ und $SR' = S$ auch $S(RR') = S$ folgt, so bilden diese r Classen eine Gruppe $\mathfrak{R}$ vom Grade r; und da das System aller h ursprünglichen Classen erster Art ebenfalls eine Gruppe $\mathfrak{H}$ bildet, welche ein Multiplum der Gruppe $\mathfrak{R}$ ist (§. 149), so ist $h = rk$, und die Gruppe $\mathfrak{H}$ zerfällt in k Complexe von der Form $\mathfrak{R}H$; alle r Classen eines solchen Complexes $\mathfrak{R}H$ geben, mit S componirt, eine und dieselbe Classe SH vom Theiler σ; und umgekehrt, wenn $SH' = SH$ ist, so folgt $SH'H^{-1} = S$, also ist $H'H^{-1} = R$ in $\mathfrak{R}$, mithin $H' = RH$ in dem Complex $\mathfrak{R}H$ enthalten. Die Anzahl h' der verschiedenen Classen vom Theiler σ ist daher $= k$, und wir sind also zu folgendem Resultate gelangt:

Die Anzahl h der ursprünglichen Classen der ersten Art ist $r$mal so gross als die Anzahl h' der Classen vom Theiler σ, wo r die Anzahl derjenigen ursprünglichen Classen der ersten Art bedeutet, welche mit der einfachsten Classe vom Theiler σ zusammengesetzt diese letztere wieder erzeugen.

Dies Resultat behält offenbar seine Gültigkeit für eine negative Determinante, auch wenn nicht alle, sondern nur die sogenannten positiven Classen gezählt werden (§. 64).

Es kommt jetzt offenbar nur noch darauf an, die Anzahl r zu bestimmen, und zu diesem Zwecke stellt *Gauss* folgenden schönen Satz auf:

Die r ursprünglichen Classen der ersten Art, welche mit der einfachsten Classe vom Theiler σ zusammengesetzt diese letztere wieder erzeugen, sind identisch mit denjenigen Classen, durch deren Formen das Quadrat des Theilers σ eigentlich oder uneigentlich dargestellt werden kann.

Um denselben zu beweisen, bemerken wir zunächst, dass man als Repräsentanten einer *jeden* ursprünglichen Classe H der ersten Art stets eine Form $(a, B, C\sigma)$ annehmen kann, in welcher a relative Primzahl zu σ ist, $2B$ und C aber durch σ theilbar sind; hat man nämlich (nach §. 93) als Repräsentanten zunächst eine Form (a, b, c) gewählt, in welcher a relative Primzahl zu σ ist, und componirt man dieselbe mit einer Form (σ, b', c') aus der einfachsten Classe S vom Theiler σ, so erhält man (§§. 146, 147) eine Form

$(a\sigma, B, C)$ vom Theiler σ, und zwar so, dass die Formen (a, b, c), (σ, b', c') resp. den Formen $(a, B, C\sigma)$, (σ, B, aC) äquivalent sind; es kann daher $(a, B, C\sigma)$ statt (a, b, c) als Repräsentant der Classe H gewählt werden.

Ist nun $SH = S$, also H eine der r Classen aus der Gruppe $\mathfrak{R}$, so ist $(a\sigma, B, C)$ äquivalent mit (σ, B, aC), und folglich existiren zwei ganze Zahlen x, y, welche der Bedingung

$$a\sigma x^2 + 2Bxy + Cy^2 = \sigma$$

genügen; hieraus folgt aber

$$a(\sigma x)^2 + 2B(\sigma x)y + C\sigma y^2 = \sigma^2,$$

d. h. σ^2 wird durch die Form $(a, B, C\sigma)$ der Classe H dargestellt, wenn den Variabeln die Werthe σx, y beigelegt werden.

Umgekehrt, ist σ^2 durch die Formen der Classe H, also auch durch die Form $(a, B, C\sigma)$ darstellbar, so existiren zwei ganze Zahlen x', y, welche der Bedingung

$$ax'^2 + 2Bx'y + C\sigma y^2 = \sigma^2$$

genügen. Zunächst ergiebt sich hieraus, dass x' durch σ theilbar sein muss; denn da C und $2B$, also auch $2By = \beta\sigma$ durch σ theilbar ist, so folgt $ax'^2 + \beta\sigma x' \equiv 0 \pmod{\sigma^2}$; ist nun δ der grösste gemeinschaftliche Divisor von $x' = \delta x$ und $\sigma = \delta\varrho$, wo also x und ϱ relative Primzahlen bedeuten, so ergiebt sich $ax^2 + \beta\varrho x \equiv 0 \pmod{\varrho^2}$, also muss ax^2, folglich auch a durch ϱ theilbar sein; da aber a relative Primzahl zu $\sigma = \delta\varrho$, also auch zu ϱ ist, so muss $\varrho = 1$, $\delta = \sigma$, also $x' = \sigma x$ sein. Nachdem dies bewiesen ist, ergiebt sich

$$a\sigma x^2 + 2Bxy + Cy^2 = \sigma;$$

da ferner $2B$ und C durch σ theilbar sind, so folgt, dass x und y relative Primzahlen sind; mithin ist σ eigentlich darstellbar durch die Form $(a\sigma, B, C)$ vom Theiler σ, welche folglich (§. 60) einer Form äquivalent sein muss, deren erster Coefficient $= \sigma$ ist, und die also der einfachsten Classe S vom Theiler σ angehört. Da nun $(a\sigma, B, C)$ auch der Classe SH angehört, so ist $SH = S$, d. h. H ist eine Classe aus der Gruppe $\mathfrak{R}$, was zu beweisen war.

Durch den hiermit bewiesenen obigen Satz sind wir nun in den Stand gesetzt, den Grad r der Gruppe $\mathfrak{R}$ genau zu bestimmen. Ist R eine Classe aus dieser Gruppe, und wird σ^2 durch ihre Formen so dargestellt, dass die beiden darstellenden Zahlen (x, y) den grössten gemeinschaftlichen Theiler δ haben, so geht δ^2 in σ^2, folg-

lich δ in $\sigma = \delta \varrho$ auf; mithin ist (nach §. 60) ϱ^2 eigentlich darstellbar durch die Formen der Classe R, und folglich kann man (nach §. 60) als Repräsentanten von R eine Form wählen, deren erster Coefficient $= \varrho^2$ ist. Da umgekehrt durch jede solche Form auch σ^2 dargestellt wird, wenn den Variabelen die Werthe $x = \delta$, $y = 0$ ertheilt werden, so gehört sie, wenn sie zugleich ursprünglich von der ersten Art ist, einer Classe R aus der Gruppe $\mathfrak{R}$ an. Wir haben mithin folgenden Satz erhalten:

Der Grad r der Gruppe $\mathfrak{R}$ ist gleich der Anzahl aller nicht äquivalenten ursprünglichen Formen der ersten Art, deren erster Coefficient ein quadratischer Divisor ϱ^2 vom Quadrate des Theilers σ ist.

Wir bemerken schliesslich, dass für jeden solchen quadratischen Divisor ϱ^2 (zufolge §. 56) nur alle diejenigen Formen zu untersuchen sind, deren mittlere Coefficienten ein vollständiges Restsystem nach dem Modulus ϱ^2 bilden.

§. 151.

Nachdem im Vorhergehenden der Weg allgemein vorgezeichnet ist, auf welchem man zur Bestimmung des Verhältnisses der Classenanzahlen h und h' gelangt, schreiten wir zur Betrachtung der speciellen Fälle, in welchen σ eine *Primzahl* ist, weil aus ihnen das allgemeine Resultat abgeleitet werden kann.

I. Ist die Determinante $D = 1 - 4n \equiv 1 \pmod{4}$, und $\sigma = 2$, so handelt es sich um die Vergleichung der Classenanzahlen der ursprünglichen Formen der ersten und zweiten Art. Bezeichnet man dieselben wieder mit h und h', so ist $h = rh'$, wo r die Anzahl der nicht äquivalenten ursprünglichen Formen erster Art bedeutet, deren erster Coefficient $= 1$ oder $= 4$ ist. Da im zweiten Fall der mittlere Coefficient ungerade sein muss, so sind nur die drei Formen

$$(1, 0, -D), \ (4, \pm 1, n)$$

in Betracht zu ziehen.

Ist $D \equiv 1 \pmod{8}$, also n gerade, so ist nur die erste dieser Formen ursprünglich von der ersten Art, folglich $r = 1$, und $h = h'$.

Ist aber $D \equiv 5 \pmod{8}$, also n ungerade, so sind alle drei Formen ursprünglich von der ersten Art, und es braucht nur noch untersucht zu werden, ob sie verschiedenen Classen angehören oder nicht. Zunächst lässt sich beweisen, dass sie entweder zu einer und derselben, oder zu drei verschiedenen Classen gehören. *Gauss* zeigt dies durch die Composition der ihnen entsprechenden Classen $1, P, Q$; da die Classen P, Q entgegengesetzt sind, so ist $PQ = 1$, und ferner lässt sich leicht zeigen, dass $PP = Q$ und $QQ = P$ ist (denn aus den beiden einigen, in P enthaltenen Formen $(4, 1, n)$, $(n, -1, 4)$ ist die Form $(4n, 2n-1, n)$ zusammengesetzt, und da diese mit $(n, 1-2n, 4n)$, $(n, 1, 4)$, $(4, -1, n)$ äquivalent ist, so folgt $PP = Q$); nimmt man nun an, dass zwei der drei Classen $1, P, Q$ identisch sind, so ergiebt sich hieraus sofort, dass auch die dritte mit ihnen übereinstimmt. Dasselbe lässt sich auch durch die folgenden Sätze erweisen.

Sind irgend zwei der drei Formen $(1, 0, -D)$, $(4, \pm 1, n)$ *äquivalent, so ist die Gleichung* $t^2 - Du^2 = 4$ *durch ungerade Zahlen* t, u *lösbar.*

Ist nämlich die erste Form mit einer der beiden anderen äquivalent, so ist (nach §. 60) der erste Coefficient 4 dieser letztern eigentlich darstellbar durch die Form $(1, 0, -D)$, also giebt es zwei relative Primzahlen t, u, welche der Gleichung $t^2 - Du^2 = 4$ genügen, woraus folgt, dass t, u, da sie nicht beide gerade sein können, nothwendig beide ungerade sein müssen. Sind ferner die beiden letzten Formen äquivalent, so giebt es (nach §. 60. Anm.) zwei ganze Zahlen x, y, welche den Bedingungen

$$4x^2 + 2xy + ny^2 = 4, \quad -2x + ny \equiv 0 \pmod{4}$$

genügen; da n ungerade ist, so muss y gerade sein $= 2u$; setzt man dann $2x + u = t$, so gehen diese Bedingungen in die folgenden über

$$t^2 - Du^2 = 4,\ t \equiv -u \pmod{4};$$

da aus der letztern $t^2 \equiv u^2 \pmod{8}$ folgt, und ausserdem $-D \equiv 3 \pmod{8}$ ist, so folgt aus der erstern $4u^2 \equiv 4 \pmod{8}$, mithin ist u, also auch t ungerade, was zu beweisen war.

Ist die Gleichung $t^2 - Du^2 = 4$ *durch ungerade Zahlen* t, u *lösbar, so sind alle drei Formen* $(1, 0, -D)$, $(4, \pm 1, n)$ *äquivalent.*

Denn wenn man t mit beliebigem Vorzeichen, dann aber $u \equiv -t \pmod{4}$ wählt, so geht die Form $(1, 0, -D)$ durch die Substitutionen

$$\begin{pmatrix} t, & \pm\frac{t+Du}{4} \\ \pm u, & \frac{t+u}{4} \end{pmatrix}$$

in die beiden Formen $(4, \pm 1, n)$ über. — Durch Verbindung der beiden vorstehenden Sätze ergiebt sich:

Die drei obigen Formen sind äquivalent oder gehören drei verschiedenen Classen an, je nachdem die Gleichung $t^2 - Du^2 = 4$ durch ungerade Zahlen t, u lösbar ist oder nicht; im ersten Falle ist $h = h'$, im zweiten $h = 3h'$.

Ist nun D positiv, so tritt der erste Fall ein oder der zweite, je nachdem die *kleinste* Lösung $t = T'$, $u = U'$ aus ungeraden oder geraden Zahlen besteht. Ist D negativ, so besitzt die Gleichung im Allgemeinen nur die beiden Auflösungen $t = \pm 2$, $u = 0$, und mithin ist $h = 3h'$; die einzige Ausnahme hiervon bildet die Determinante $D = -3$, weil die Gleichung ausser den beiden Lösungen $t^2 = 4$, $u = 0$ noch die vier Lösungen $t^2 = u^2 = 1$ besitzt, und folglich ist in diesem Falle wieder $h = h'$.

Diese Resultate stimmen vollkommen mit denjenigen überein, welche wir früher (§§. 97, 99) mit Hülfe ganz anderer Principien abgeleitet haben.

II. Ist $D = D'\sigma^2$, so leuchtet ein, dass h' zugleich die Anzahl der ursprünglichen Classen erster Art von der Determinante D' ist. Unter der Voraussetzung, dass σ eine Primzahl ist, haben wir, um das Verhältniss $r = h : h'$ zu bestimmen, nur die l Formen

$$(1, 0, -D) \quad \text{und} \quad (\sigma^2, B\sigma, BB - D') \tag{1}$$

zu betrachten, wo B ein vollständiges Restsystem (mod. σ) durchlaufen muss, mit Ausnahme derjenigen Werthe, für welche $BB \equiv D'$ (mod. σ) wird, weil diesen keine ursprünglichen Formen entsprechen; die Anzahl der zu betrachtenden ursprünglichen Formen ist daher

$$l = 2 \quad \text{oder} \quad \sigma - \left(\frac{D'}{\sigma}\right) \tag{2}$$

je nachdem $\sigma = 2$ oder eine ungerade Primzahl ist. Zur Bestimmung der Anzahl r der verschiedenen Classen, welchen diese l Formen angehören, gelangen wir durch die folgenden Sätze.

Die beiden Formen $(1, 0, -D)$, $(\sigma^2, \beta\sigma, \beta\beta - D')$ *sind stets und nur dann äquivalent, wenn es zwei ganze Zahlen* t', u' *giebt, welche den Bedingungen*

$$t't' - D'u'u' = 1, \quad t' + \beta u' \equiv 0 \pmod{\sigma} \tag{3}$$

genügen; zwei Formen $(\sigma^2, b\sigma, bb - D')$, $(\sigma^2, b'\sigma, b'b' - D')$ *sind stets und nur dann äquivalent, wenn es zwei ganze Zahlen* t', u' *giebt, welche den Bedingungen*

$$t't' - D'u'u' = 1, \; (b - b')t' + (bb' - D')u' \equiv 0 \pmod{\sigma} \tag{4}$$

genügen.

Die Aequivalenz der Formen $(1, 0, -D)$, $(\sigma^2, \beta\sigma, \beta\beta - D')$ ist (nach §. 60 Anmerkung) gleichbedeutend mit der Annahme der Existenz zweier ganzen Zahlen x, y, welche die Bedingungen

$$x^2 - D'\sigma^2 y^2 = \sigma^2,$$
$$x + \beta\sigma y \equiv 0, \; -\beta\sigma x - D'\sigma^2 y \equiv 0 \pmod{\sigma^2}$$

erfüllen; da nun aus der ersten folgt, dass x durch σ theilbar ist, und da sie durch die Substitutionen $x = \sigma t'$, $y = u'$ in die Bedingungen (3) übergehen, aus welchen sie umgekehrt folgen, so ist der erste Theil des Satzes erwiesen. Ebenso fällt die Annahme der Aequivalenz der Formen $(\sigma^2, b\sigma, bb - D')$, $(\sigma^2, b'\sigma, b'b' - D')$ zusammen mit der Annahme der Existenz zweier ganzen Zahlen x, y, welche die Bedingungen

$$\sigma^2 x^2 + 2b\sigma xy + (bb - D')y^2 = \sigma^2,$$
$$\sigma^2 x + (b + b')\sigma y \equiv 0, \; (b - b')\sigma x + (bb - D')y \equiv 0 \pmod{\sigma^2}$$

befriedigen; da nun der Voraussetzung nach $bb - D'$ nicht durch σ theilbar ist, so muss y^2 und folglich auch y durch die Primzahl σ theilbar sein; da ferner die vorstehenden Bedingungen durch die Substitution $y = \sigma u'$, $x = t' - bu'$ in die Bedingungen (4) übergehen, aus denen sie auch rückwärts folgen, so ist auch der zweite Theil des obigen Satzes bewiesen.

Bedeutet λ *die Anzahl derjenigen Formen* (1), *welche der Hauptclasse angehören, so ist* $l = r\lambda$.

Gehört die Form $(\sigma^2, \beta\sigma, \beta^2 - D')$ der Hauptclasse an, so existirt eine Lösung (t', u') der Gleichung

$$t't' - D'u'u' = 1 \tag{5}$$

welche der Congruenz $t' + \beta u' \equiv 0 \pmod{\sigma}$ genügt, und folglich kann u' nicht durch σ theilbar sein. Ist umgekehrt (t', u') eine Lösung der Gleichung (5), und u' nicht theilbar durch σ, so existirt

stets eine und nur eine Zahlclasse β (mod. σ), welche der Congruenz $t' + \beta u' \equiv 0$ (mod. σ) genügt, und ihr entspricht eine zur Hauptclasse gehörige Form $(\sigma^2, \beta\sigma, \beta^2 - D')$. Um also alle diese Formen zu erhalten, muss man alle Lösungen (t', u') der Gleichung (5) aufstellen, in welchen u' nicht durch σ theilbar ist, und jedesmal die entsprechende Zahlclasse β (mod. σ) durch die Congruenz $t' + \beta u' \equiv 0$ (mod. σ) bestimmen. Da ausserdem die Form $(1, 0, -D)$ zur Hauptclasse gehört, und λ die Anzahl aller zur Hauptclasse gehörenden Formen (1) bedeutet, so ist also $\lambda - 1$ die Anzahl der sämmtlichen incongruenten Zahlclassen β (mod. σ), welche aus Lösungen (t', u') der Gleichung (5) vermöge der Congruenz $t' + \beta u' \equiv 0$ (mod. σ) erzeugt werden können.

Sind hierdurch schon alle Formen (1) erschöpft, so ist $l = \lambda$ und $r = 1$, also der Satz richtig. Giebt es aber eine nicht zur Hauptclasse gehörende ursprüngliche Form $(\sigma^2, b'\sigma, b'b' - D')$, d.h. giebt es eine von den $\lambda - 1$ Zahlclassen β (mod. σ) verschiedene Zahlclasse b' von der Beschaffenheit, dass $b'b' - D'$ nicht durch σ theilbar ist, so wollen wir zeigen, dass unter den l Formen (1) sich genau $(\lambda - 1)$ Formen $(\sigma^2, b\sigma, bb - D')$ finden, welche alle mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalent und von ihr verschieden sind. Ist nämlich $(\sigma^2, b\sigma, bb - D')$ eine solche Form, also $b - b'$ nicht durch σ theilbar, so giebt es, wie oben gezeigt ist, eine Lösung (t', u') der Gleichung (5), welche der Congruenz

$$(b - b')t' + (bb' - D')u' \equiv 0 \text{ (mod. } \sigma) \qquad (4)$$

genügt, aus welcher zugleich folgt, dass u' nicht durch σ theilbar ist. Umgekehrt, ist (t', u') eine Lösung der Gleichung (5), in welcher u' nicht durch σ theilbar ist, und $t' + \beta u' \equiv 0$ (mod. σ), so existirt, weil $b' - \beta$ nicht durch σ theilbar ist, immer eine und nur eine Zahlclasse b (mod. σ), welche die Congruenz

$$(b' - \beta)\, b \equiv D' - b'\beta \text{ (mod. } \sigma) \qquad (6)$$

befriedigt, und zwar kann b nicht $\equiv b'$ (mod. σ) sein, weil hieraus $b'b' \equiv D'$ (mod. σ) folgen würde; multiplicirt man nun (6) mit u', so ergiebt sich (4), und folglich ist wirklich $(\sigma^2, b\sigma, bb - D')$ äquivalent mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ und zugleich verschieden von ihr, weil $b - b'$ nicht durch σ theilbar ist. Um also alle mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalenten und von ihr verschiedenen Formen $(\sigma^2, b\sigma, bb - D')$ zu erhalten, braucht man nur die sämmtlichen $(\lambda - 1)$ Congruenzen (6) aufzustellen, welche den $(\lambda - 1)$ incongruenten Zahlclassen β (mod. σ) entsprechen, und für

jede die entsprechende Zahlclasse b zu bestimmen. Auf diese Weise entstehen aber wirklich auch $(\lambda - 1)$ verschiedene Zahlclassen $b \pmod{\sigma}$; denn wollte man annehmen, es könnte zwei verschiedenen Zahlclassen β, β' (mod. σ) eine und dieselbe Zahlclasse b (mod. σ) entsprechen, so wäre

$$(b' - \beta) b \equiv D' - b'\beta, \; (b' - \beta') b \equiv D' - b'\beta' \pmod{\sigma};$$

hieraus würde aber durch Subtraction $(\beta' - \beta)(b - b') \equiv 0 \pmod{\sigma}$ folgen, was unmöglich ist, da weder $\beta' - \beta$ noch $b - b'$ durch σ theilbar ist. Mithin giebt es wirklich genau $\lambda - 1$ verschiedene Formen $(\sigma^2, b\sigma, bb - D')$, welche mit der Form $(\sigma^2, b'\sigma, b'b' - D')$ äquivalent und zugleich von ihr verschieden sind. Von den l Formen (1) gehören daher immer je λ, und nicht mehr, zu einer und derselben Classe, folglich ist $l = r\lambda$, was zu beweisen war.

Ist die Determinante $D = D'\sigma^2$ negativ, so ist h im Allgemeinen $= lh'$, und nur dann $= \frac{1}{2} lh'$, wenn $D' = -1$.

Denn die Gleichung (5) besitzt nur im letztern Falle Lösungen $(t' = 0, u' = \pm 1)$, in welchen u' nicht durch σ theilbar ist; da denselben nur die eine Zahlclasse $\beta \equiv 0 \pmod{\sigma}$ entspricht, so ist $\lambda = 2$, also $r = \frac{1}{2} l$; in allen anderen Fällen ist $\lambda = 1$, also $r = l$.

Ist die Determinante $D = D'\sigma^2$ positiv, so ist $h \log (T + U\sqrt{D})$ $= l . h' \log (T' + U'\sqrt{D'})$, wo (T, U), (T', U') resp. die kleinsten positiven Auflösungen der Gleichungen $T^2 - DU^2 = 1$, $T'^2 - D'U'^2 = 1$ bedeuten.

Um dies zu beweisen, schicken wir eine Bemerkung über die Lösungen der Gleichung (5) voraus. Wenn zwei solche Lösungen (t', u'), (t'', u'') der Bedingung

$$t'u'' - u't'' \equiv 0 \pmod{\sigma} \tag{7}$$

genügen, so kann man, wenn $\sqrt{D'}$ und $\sqrt{D} = \sigma\sqrt{D'}$ immer positiv genommen werden,

$$t' + u'\sqrt{D'} = (t'' + u''\sqrt{D'})(t + u\sqrt{D}), \tag{8}$$

setzen, wo die ganzen Zahlen t, u eine Lösung der Gleichung

$$t^2 - Du^2 = 1 \tag{9}$$

bilden. Umgekehrt, sind (t'', u''), (t, u) resp. Lösungen der Gleichungen (5), (9), so liefert die Gleichung (8) stets eine Lösung (t', u') der Gleichung (5), welche zugleich der Bedingung (7) genügt. Je zwei solche Lösungen (t', u'), (t'', u'') der Gleichung (5) wollen wir äquivalent nennen; dann leuchtet sofort ein, dass zwei Lö-

sungen, welche einer dritten äquivalent sind, auch einander äquivalent sein müssen. Man kann daher die sämmtlichen Lösungen der Gleichung (5) in Classen eintheilen, deren jede alle und nur solche Lösungen enthält, die unter einander äquivalent sind. Da nun die Gleichung (8) lehrt, aus einer gegebenen Lösung (t'', u'') alle ihr äquivalenten Lösungen (t', u') zu finden, und da $t + u\sqrt{D} = \pm (T + U\sqrt{D})^n$ ist, wo das Vorzeichen nach Belieben, und für n jede ganze Zahl gewählt werden darf (§. 85), so leuchtet ein (vergl. §. 87), dass aus jeder Classe von Lösungen ein und nur ein Repräsentant (t', u') so gewählt werden kann, dass

$$1 \leqq t' + u'\sqrt{D'} < T + U\sqrt{D}$$

wird; da ferner $(T, U\sigma)$ ebenfalls eine Lösung der Gleichung (5), und folglich (§. 85)

$$T + U\sqrt{D} = (T' + U'\sqrt{D'})^{\lambda'}$$

ist, wo λ' eine bestimmte positive ganze Zahl bedeutet, so leuchtet ein, dass die ersten Factoren $t' + u'\sqrt{D'}$ der obigen Repräsentanten (t', u') von der Form $(T' + U'\sqrt{D'})^{n'}$ sind, wo n' die λ' Werthe $0, 1, 2 \ldots (\lambda' - 1)$ durchlaufen muss, dass also die Anzahl der Classen $= \lambda'$ ist.

Die erste von diesen Classen enthält also die Lösungen (t', u') und nur solche, deren zweite Elemente u' durch σ theilbar sind. Jede Lösung (t', u') aus einer der übrigen $\lambda' - 1$ Classen liefert aber durch die Congruenz $t' + \beta u' \equiv 0 \pmod{\sigma}$ eine zugehörige Zahlclasse $\beta \pmod{\sigma}$, und da unmittelbar einleuchtet, dass zwei solche Lösungen stets und nur dann zu derselben Zahlclasse $\beta \pmod{\sigma}$ führen, wenn sie derselben Classe von Lösungen angehören, so muss die Anzahl $\lambda - 1$ der Zahlclassen β mit der Anzahl $\lambda' - 1$ dieser Classen von Lösungen übereinstimmen; also ist $\lambda = \lambda'$, was zu beweisen war.

Offenbar lässt sich aus dem hier behandelten speciellen Fall ohne Schwierigkeit das in §. 100 erhaltene Resultat für den allgemeinen Fall ableiten, in welchem σ eine beliebige zusammengesetzte Zahl ist.

§. 152.

Wir beschränken uns nun im Folgenden auf die Composition von ursprünglichen Classen erster Art, und behalten ausserdem, wenn die Determinante D negativ ist, nur die positiven Classen bei, deren Zusammensetzung offenbar immer wieder zu positiven Classen führt. Diese h Classen, welche eine Gruppe $\mathfrak{H}$ bilden, zerfallen (§. 122) je nach dem Ausfall der λ Charaktere C, welche dieser Determinante D entsprechen, in Geschlechter, und es ist mit Hülfe des Reciprocitätssatzes gezeigt (§. 123), dass *höchstens* der Hälfte aller angebbaren Totalcharaktere wirklich existirende Classen entsprechen. *Gauss**) leitet nun diesen letzteren Satz aus der Theorie der Composition ab, und er benutzt ihn, um darauf einen neuen, den *zweiten* Beweis des Reciprocitätssatzes zu gründen. Da diese tiefsinnigen Principien sich auf die Beweise von höheren Reciprocitätsgesetzen übertragen lassen**), so theilen wir dieselben in diesem und den folgenden Paragraphen mit.

Sind ε, ε' die Werthe eines Charakters C resp. für die Classen H, H', so ist $C = \varepsilon\varepsilon'$ für die Classe HH'.

Man kann als Repräsentanten der Classen H, H' immer zwei einige Formen nehmen, deren erste Coefficienten a, a' relative Primzahlen zu $2D$ sind; da die aus ihnen zusammengesetzte, also der Classe HH' angehörende Form den ersten Coefficienten aa' hat, welcher ebenfalls relative Primzahl zu $2D$ ist, so ergiebt sich der zu beweisende Satz unmittelbar, wenn man bedenkt, dass der Charakter C oder $C(n)$ ein Ausdruck von der Art

$$(-1)^{\frac{1}{2}(n-1)},\ (-1)^{\frac{1}{8}(n^2-1)},\ (-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)},\ \left(\frac{n}{l}\right)\cdots$$

ist (§. 122), und dass folglich die drei Werthe $C(a)$, $C(a')$, $C(aa')$, welche dieser Charakter resp. in den drei Classen H, H', HH' besitzt, der Bedingung $C(a)\,C(a') = C(aa')$ genügen.

Aus diesem Satze ergiebt sich, dass, wenn die Classen K, K' resp. denselben Geschlechtern G, G' angehören, wie die Classen

*) *D. A.* artt. 257 — 262.

**) *Kummer: Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist.* 1859. Vergl. Berliner Monatsbericht vom 18. Febr. 1858.

H, H', dann auch die Classen KK' und HH' sich in einem und demselben Geschlechte finden, welches das *aus* G, G' *zusammengesetzte Geschlecht* heissen soll*). Sind ferner N, N' zwei Classen des *Hauptgeschlechtes*, d. h. desjenigen Geschlechtes, in welchem sich die Hauptform $(1, 0, -D)$ findet, und folglich alle Charaktere C den Werth $+1$ haben, so gehört die zusammengesetzte Classe NN' ebenfalls diesem Geschlechte an, mithin bilden alle n Classen des Hauptgeschlechtes eine Gruppe $\mathfrak{N}$ vom Grade n (§. 149); zugleich zerfallen die sämmtlichen h Classen in g Complexe $\mathfrak{N}H$ von je n Classen, welche jedesmal einem und demselben Geschlecht angehören; zwei verschiedene solche Complexe gehören, wie man leicht erkennt, auch zu verschiedenen Geschlechtern; mithin ist $h = ng$, und g die Anzahl der wirklich existirenden von einander verschiedenen Geschlechter**).

Die Determinante D heisst *regulär* oder *irregulär*, je nachdem die von den n Classen des Hauptgeschlechtes gebildete Gruppe regulär ist oder nicht (§. 149); bedeutet im letztern Falle δ den Grad der grössten in ihr enthaltenen regulären Gruppe, so heisst die ganze Zahl $n:\delta$ der *Irregularitätsexponent* der Determinante***).

Aus dem obigen Satze über den Charakter einer zusammengesetzten Classe ergiebt sich ferner unmittelbar der folgende:

Jede Classe Q, welche durch Duplication einer Classe entsteht, gehört dem Hauptgeschlechte an.

Die Anzahl q der verschiedenen Classen Q, welche durch Duplication der sämmtlichen h Classen entstehen, ist daher $\leqq n$ (da diese Classen, wie leicht zu ersehen ist, eine Gruppe $\mathfrak{Q}$ bilden, so muss q gewiss ein Divisor von n sein). Um sie genauer zu bestimmen, nehmen wir an, Q entstehe durch Duplication der bestimmten Classe H, und fragen nach allen Classen H', durch deren Duplication dieselbe Classe Q entsteht. Aus der Annahme $H'H' = Q = HH$ folgt nun, wenn man $H' = AH$ setzt, $AA = 1$, also $A = A^{-1}$, d. h. die Classe A ist identisch mit der ihr entgegengesetzten Classe, und folglich ist sie eine *ambige* Classe (§. 148, 2., §§. 56 — 58). Umgekehrt, ist $H' = AH$, und A eine ambige Classe, so ist auch $H'H' = HH$. Schreibt man daher alle α ambigen Classen A auf, welche offenbar eine Gruppe $\mathfrak{A}$ bilden, so zerfallen alle h Classen

*) *Gauss: D. A.* artt. 246, 247.

**) *Gauss: D. A.* art. 252.

***) *Gauss: D. A.* art. 306. VII.

in q Complexe $\mathfrak{A}H$ von je α Classen, deren Duplication eine und dieselbe Classe HH hervorbringt, während zwei Classen, welche zwei verschiedenen solchen Complexen angehören, durch Duplication auch zwei verschiedene Classen hervorbringen; und endlich ist $h = \alpha q$.

Da nun h auch $= ng$, und ausserdem $q \leqq n$ ist, so ergiebt sich $g \leqq \alpha$, d. h. der Satz: *Die Anzahl der wirklich existirenden verschiedenen Geschlechter ist höchstens gleich der Anzahl der ambigen Classen.*

§. 153.

Es kommt also jetzt darauf an, für eine gegebene Determinante D die Anzahl α aller ambigen Classen A genau zu bestimmen, welche ursprünglich von erster Art sind.

Da in jeder ambigen Classe $A = A^{-1}$ stets mindestens eine ambige Form (a, b, c) zu finden ist (§. 58), so bleibt gewiss keine jener α Classen unvertreten, wenn wir alle ambigen Formen aufschreiben. Da nun in einer solchen Form $2b$ durch a theilbar, folglich b entweder $\equiv 0$, oder $\equiv \frac{1}{2}a$ (mod. a), also (a, b, c) selbst mit einer Form äquivalent ist (§. 56), deren mittlerer Coefficient entweder Null, oder die Hälfte des ersten Coefficienten ist, so genügt es, alle Formen

$$\left(a,\ 0,\ \frac{-D}{a}\right) \quad \text{und} \quad \left(2b,\ b,\ \frac{b^2 - D}{2b}\right)$$

zu betrachten, welche ursprünglich von erster Art sind.

Bedeutet μ die Anzahl aller verschiedenen *ungeraden* Primzahlen, welche in D aufgehen, ist ferner $\nu = 0$ oder $= 1$, je nachdem D ungerade oder gerade, so ist $\mu + \nu$ die Anzahl *aller* verschiedenen in D aufgehenden Primzahlen. Dann leuchtet ein, dass die Anzahl aller ursprünglichen Formen vom Typus

$$(a,\ 0,\ a')$$

gleich $2^{\mu+\nu+1}$ ist; die eine Hälfte derselben hat positive erste Coefficienten, die andere Hälfte negative.

Betrachten wir nun die anderen ambigen ursprünglichen Formen erster Art, deren Typus

$$\left(2b,\ b,\ \frac{b^2-D}{2b}\right)$$

ist, so muss b ein solcher Divisor von $D = -bb'$ sein, dass der dritte Coefficient $\frac{1}{2}(b+b')$ eine ganze Zahl und relative Primzahl zu $2b$ wird; mithin muss zunächst $b + b' \equiv 2$ (mod. 4) sein, und ferner dürfen b und b' keinen gemeinschaftlichen ungeraden Divisor haben. Sind nun b und b' ungerade, so folgt $b' \equiv b$, $D \equiv -bb \equiv 3$ (mod. 4); umgekehrt, wenn $D \equiv 3$ (mod. 4), so kann b nur ungerade sein, und aus $bb' = -D \equiv 1$ (mod. 4) folgt von selbst, dass $b \equiv b'$, also $b + b' \equiv 2$ (mod. 4) wird; mithin kann b jeder Divisor von D sein, für welchen b und b' relative Primzahlen werden. Die Anzahl dieser Formen

$$(2b,\ b,\ \tfrac{1}{2}(b+b'))$$

ist daher $= 2^{\mu+1}$, unter welchen ebensoviele mit positiven, wie mit negativen ersten Coefficienten vorkommen. Sind aber b und b' gerade, so ist eine von ihnen $\equiv 0$, die andere $\equiv 2$ (mod. 4), mithin $D \equiv 0$ (mod. 8), und $\frac{1}{2}b$, $\frac{1}{2}b'$ sind relative Primzahlen. Umgekehrt, wenn $D \equiv 0$ (mod. 8) ist, so muss b gerade sein, und man kann für $\frac{1}{2}b$ jeden Divisor von $\frac{1}{4}D = -\frac{1}{2}b \cdot \frac{1}{2}b'$ wählen, für welchen $\frac{1}{2}b$, $\frac{1}{2}b'$ relative Primzahlen werden; mithin ist die Anzahl dieser Formen, da $\frac{1}{4}D$ gerade ist, gleich $2^{\mu+2}$, und unter ihnen finden sich ebensoviele mit positiven wie mit negativen ersten Coefficienten.

Die Anzahl aller dieser ambigen ursprünglichen Formen erster Art ist daher gleich

$$\begin{array}{lll} 2^{\mu+1}, & \text{wenn} & D \equiv 1 \text{ (mod. 4)}, \\ 2^{\mu+2}, & \text{„} & D \equiv 2, 3, 4, 6, 7 \text{ (mod. 8)}, \\ 2^{\mu+3}, & \text{„} & D \equiv 0 \text{ (mod. 8)}; \end{array}$$

sie ist folglich in allen Fällen genau doppelt so gross, als die Anzahl $2^\lambda = 2\tau$ aller angebbaren Totalcharaktere für die Determinante D (§. 122). Es kommt jetzt darauf an, die Anzahl der verschiedenen Classen zu bestimmen, welche durch diese Formen repräsentirt werden.

Sieht man von dem singulären Fall $D = -1$ vorläufig ganz ab, so erkennt man leicht, dass die Coefficienten a und a', ebenso die Zahlen b und b', selbst ihren absoluten Werthen nach, von einander verschieden sein müssen. Hätten nämlich die relativen Primzahlen a, a' denselben absoluten Werth 1, so wäre $D = \pm 1$; dasselbe würde sich ergeben, wenn man annehmen wollte, die unge-

raden Zahlen b und b' hätten denselben absoluten Werth; sind endlich b und b' gerade, so ist die eine der Zahlen $\frac{1}{2}b$, $\frac{1}{2}b'$ gerade, die andere ungerade, also haben sie verschiedene absolute Werthe. Hieraus folgt, dass die sämmtlichen obigen Formen immer in Paare von je zwei von einander verschiedenen Formen $(a, 0, a')$, $(a', 0, a)$, und $(2b, b, \frac{1}{2}(b+b'))$, $(2b', b', \frac{1}{2}(b+b'))$ zerfallen, und da die erste resp. durch die Substitutionen $\binom{0,\ 1}{-1,\ 0}$, $\binom{-1,\ -1}{+2,\ +1}$ in die zweite übergeht, so genügt es, diejenige von ihnen beizubehalten, deren erster Coefficient der kleinere ist; mithin haben wir nur noch 2τ Formen $(a, 0, a')$, $(2b, b, \frac{1}{2}(b+b'))$, in welchen die absoluten Werthe (a) und $(b) < \sqrt{(D)}$ sind; und unter diesen Formen giebt es wieder ebensoviele mit positiven ersten Coefficienten, wie mit negativen.

Ist nun D *negativ*, so behalten wir nur die τ Formen bei, deren äussere Coefficienten positiv sind, und wir wollen zeigen, dass sie die Repräsentanten von ebensovielen verschiedenen Classen sind. Zunächst sind alle Formen $(a, 0, a')$ und diejenigen Formen $(2b, b, \frac{1}{2}(b+b'))$, in welchen $3b \leqq b'$ ist, *reducirt* (§. 64), und statt jeder nicht reducirten Form $(2b, b, \frac{1}{2}(b+b'))$, in welcher also $3b > b'$, können wir die ihr nach rechts benachbarte reducirte Form $(\frac{1}{2}(b+b'), \frac{1}{2}(b'-b), \frac{1}{2}(b+b'))$ substituiren. Man erkennt nun leicht, dass alle diese τ reducirten Formen von einander verschieden, und dass auch keine zwei einander entgegengesetzt sind, weil keiner der mittleren Coefficienten negativ ist; sie gehören daher (§. 65) ebensovielen verschiedenen Classen an. Wir haben daher das Resultat: *Die Anzahl α aller positiven ambigen ursprünglichen Classen erster Art von negativer Determinante D ist halb so gross wie die Anzahl 2τ aller angebbaren Totalcharaktere.* Dies gilt offenbar auch noch für den oben ausgeschlossenen singulären Fall $D = -1$, da die beiden Formen $(1, 0, 1)$, $(2, 1, 1)$ äquivalent sind.

Ist aber die Determinante D *positiv*, so entspricht jeder der obigen 2τ ambigen Formen (A, B, C) eine einzige ihr äquivalente ambige Form (A, B', C'), wo B' durch die Bedingungen

$$B' \equiv B \text{ (mod. } A), \quad 0 < \sqrt{D} - B' < (A)$$

vollständig bestimmt ist; offenbar entstehen auf diese Weise wieder 2τ ambige und von einander verschiedene Formen (A, B', C'). Um nun zu zeigen, dass alle diese Formen zugleich *reducirt* sind (§. 74), braucht nur nachgewiesen zu werden, dass $(A) < \sqrt{D} + B'$ ist; wenn $(A) < \sqrt{D}$ ist, so folgt dies unmittelbar daraus, dass zufolge der obigen Grenzbedingungen B' positiv ist; wenn aber $(A) > \sqrt{D}$

ist, was nur bei den Formen des zweiten Typus eintreten kann, so ist $A = 2B$, und $(B) < \sqrt{D}$, folglich $B' = (B)$, weil dieser Werth allen an B' gestellten Forderungen genügt, und also wieder $(A) < \sqrt{D} + B'$. Endlich behaupten wir, dass jede ambige reducirte Form (a, b, c), welche zugleich ursprünglich von erster Art ist, nothwendig mit einer dieser 2τ Formen (A, B', C') identisch sein muss; ist nämlich b theilbar durch a, so muss $(a) < \sqrt{D}$ sein, weil in einer reducirten Form $0 < b < \sqrt{D}$ ist, und die mit (a, b, c) äquivalente Form $(a, 0, a')$ ist eine der 2τ Formen (A, B, C), woraus folgt, dass (a, b, c) selbst mit der entsprechenden Form (A, B', C') identisch sein muss, weil b als mittlerer Coefficient einer reducirten Form denselben charakteristischen Bedingungen genügt, wie B'; ist aber b nicht theilbar durch a, so ist wenigstens $(a) < 2\sqrt{D}$, und folglich die mit (a, b, c) äquivalente Form $(a, \frac{1}{2}a, c')$ eine der Formen (A, B, C), woraus wieder folgt, dass (a, b, c) mit der entsprechenden Form (A, B', C') identisch ist. Wir müssen aus dem Vorhergehenden schliessen, dass die Anzahl aller ambigen ursprünglichen Formen erster Art, welche zugleich reducirt sind, genau $= 2\tau$ ist; da nun in jeder ambigen Classe sich stets zwei und nur zwei solche Formen finden (§§. 78, 82), so erhalten wir dasselbe Resultat, wie für negative Determinanten: *Die Anzahl α aller ambigen ursprünglichen Classen erster Art von positiver Determinante D ist genau halb so gross wie die Anzahl 2τ aller angebbaren Totalcharaktere.*

Verbinden wir diese Resultate mit dem des vorigen Paragraphen, so ergiebt sich folgender Satz*):

Die Anzahl der wirklich existirenden verschiedenen Geschlechter ist höchstens halb so gross wie die Anzahl der angebbaren Totalcharaktere.

§. 154.

Das soeben erhaltene Resultat führt nun zu einem neuen Beweise des Reciprocitätssatzes, sowie der Ergänzungssätze über den Charakter der Zahlen -1 und 2. Wir machen zunächst die Be-

*) Vergl. §. 123.

merkung, dass in den Fällen $D = -1, \pm 2$, und wenn $D \equiv 1 \pmod{4}$ eine positive oder negative Primzahl ist, nur ein einziger Charakter C (§. 122), und folglich (§. 153) nur ein einziges Geschlecht vorhanden ist, welches kein anderes, als das durch die Form $(1, 0, -D)$ vertretene Hauptgeschlecht $(C = +1)$ sein kann. Wir bezeichnen nun mit p, q immer positive, ungerade (von einander verschiedene) Primzahlen, und wenden uns zum Beweise der drei Sätze:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$$
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$

1. Ist zunächst $p \equiv 1 \pmod{4}$, so ist $(-1, 0, p)$ eine ursprüngliche Form erster Art von der Determinante $D = p \equiv 1 \pmod{4}$, für welche nur Formen existiren, die dem Hauptgeschlecht angehören; mithin muss der Coefficient -1 quadratischer Rest von p sein. Ist aber $p \equiv 3 \pmod{4}$, so ist -1 Nichtrest von p; wäre nämlich $-1 = b^2 - cp$, so wäre (p, b, c) eine (positive) Form der Determinante $D = -1$, welche zufolge ihres Coefficienten p den Charakter $C = -1$ besässe, was unmöglich ist.

2. Ist $p \equiv 1 \pmod{8}$, so ist $(8, 1, \frac{1}{8}(1-p))$ oder $(8, 3, \frac{1}{8}(9-p))$, je nachdem $p \equiv 9$ oder $\equiv 1 \pmod{16}$ ist, eine ursprüngliche Form erster Art von der Determinante $D = p \equiv 1 \pmod{4}$, und muss deshalb dem Hauptgeschlecht angehören, woraus folgt, dass 8 und also auch 2 quadratischer Rest von p ist.

Ist ferner $p \equiv 7 \pmod{8}$, so ist 2 ebenfalls quadratischer Rest von p; denn im entgegengesetzten Fall wäre (zufolge 1. und §. 33, III.) die Zahl -2 Rest von p, also $-2 = b^2 - cp$, und es existirte eine (positive) Form (p, b, c) der Determinante $D = -2$, für welche $C = -1$ wäre, was unmöglich ist.

Ist endlich $p \equiv 3$ oder $5 \pmod{8}$, so ist 2 Nichtrest von p; wäre nämlich $2 = b^2 - cp$, so wäre (p, b, c) eine Form der Determinante $D = 2$, für welche $C = -1$ wäre, was unmöglich ist.

3. Ist wenigstens eine der beiden Primzahlen p, q, z. B. $p \equiv 1 \pmod{4}$, so ist

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Ist nämlich q Rest von p, so gilt Dasselbe von $-q$ (zufolge 1. und §. 33, I.), mithin kann man, nachdem man das Vorzeichen $\pm$ so gewählt hat, dass $\pm q \equiv 1 \pmod{4}$ wird, immer $\pm q = b^2 - cp$ setzen, und folglich ist (p, b, c) eine ursprüngliche Form erster Art von der Determinante $D = \pm q \equiv 1 \pmod{4}$, und zwar eine positive, wenn D negativ ist; sie gehört also dem Hauptgeschlechte an, und folglich ist p Rest von q. Ist aber q Nichtrest von p, so muss auch p Nichtrest von q sein, weil im entgegengesetzten Falle $p = b^2 - cq$ wäre, also eine ursprüngliche Form erster Art (q, b, c) der Determinante $D = p \equiv 1 \pmod{4}$ existirte, für welche $C = -1$ wäre, was unmöglich ist.

Sind aber beide Primzahlen $p, q \equiv 3 \pmod{4}$, so ist

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Dies ergiebt sich am einfachsten durch die Betrachtung der Determinante $D = pq \equiv 1 \pmod{4}$, für welche zwei Charaktere C, also höchstens zwei verschiedene Geschlechter existiren. Da nun die beiden ursprünglichen Formen $(1, 0, -pq)$, $(-1, 0, pq)$ erster Art (zufolge 1.) wirklich zwei verschiedenen Geschlechtern angehören, so muss jede andere ursprüngliche Form erster Art von derselben Determinante, z. B. die Form $(p, 0, -q)$ einem der durch diese beiden Formen repräsentirten Geschlechter angehören. Gehört sie in das Hauptgeschlecht, so ist gleichzeitig p Rest von q, und $-q$ Rest von p, folglich (nach 1.) q Nichtrest von p; gehört sie aber in dasselbe Geschlecht wie die Form $(-1, 0, pq)$, so ist gleichzeitig p Nichtrest von q, und $-q$ Nichtrest von p, folglich q Rest von p. Was zu beweisen war.

§. 155.

Mit Hülfe des so von Neuem bewiesenen Reciprocitätssatzes lässt sich nun wieder, wie in §. 123 geschehen ist, darthun, dass höchstens diejenigen τ Geschlechter existiren können, deren Totalcharaktere der dortigen Bedingung $\Pi\, C' = +1$ genügen; dass aber alle diese τ Geschlechter wirklich existiren (§. 125), hat *Gauss* mit Hülfe der von ihm gegründeten Theorie der ternären quadratischen Formen

$$Ax^2 + By^2 + Cz^2 + 2A'yz + 2B'zx + 2C'xy$$

bewiesen*). Da oben (§. 152) gezeigt ist, dass $ng = \alpha q$ ist, wo g die Anzahl der wirklich existirenden Geschlechter, n die Anzahl der in jedem derselben enthaltenen Classen, $\alpha = \tau$ die Anzahl der ambigen Classen oder also die Anzahl der Totalcharaktere, welche der Bedingung $\Pi C' = +1$ genügen, und q die Anzahl der durch Duplication entstehenden Classen bedeutet, so leuchtet ein, dass der zu beweisende Satz $g = \alpha$ wesentlich identisch ist mit dem Satze $n = q$; da ferner n die Anzahl aller Classen des Hauptgeschlechtes ist, und jede der durch Duplication entstehenden q Classen gewiss dem Hauptgeschlechte angehört (§. 152), so ist der zu beweisende Satz wesentlich identisch mit dem folgenden**):

Jede Classe des Hauptgeschlechtes entsteht durch Duplication.

Wir können hier unmöglich darauf eingehen, den Beweis mitzutheilen, welchen *Gauss* auf die Theorie der ternären Formen gestützt hat; da dieses tiefe Theorem aber den schönsten Abschluss der Lehre von der Composition bildet, so können wir es uns nicht versagen, dasselbe auch ohne Hülfe der Dirichlet'schen Principien auf einem Wege abzuleiten, der zugleich die Grundlage für andere wichtige Untersuchungen bildet.

Um einen bestimmten Boden für diese Untersuchung zu gewinnen, heben wir zunächst eine charakteristische Eigenschaft aller der Classen Q hervor, welche durch Duplication entstehen: *alle Formen dieser Classen und nur diese Formen sind fähig, Quadratzahlen darzustellen, welche relative Primzahlen zu* $2D$ *sind.* Entsteht nämlich Q durch Duplication einer Classe K, so kann man aus K immer eine solche Form auswählen, deren erster Coefficient x relative Primzahl zu $2D$ ist; da alsdann diese Form mit sich selbst einig ist, so entsteht durch Duplication eine der Classe Q angehörige Form, deren erster Coefficient $= x^2$ ist, und folglich ist diese Quadratzahl durch die Formen der Classe Q eigentlich darstellbar. Umgekehrt, ist Q eine Classe, durch deren Formen eine Quadratzahl dargestellt werden kann, welche relative Primzahl zu $2D$ ist, so giebt es auch eine solche Quadratzahl x^2, welche durch diese Formen *eigentlich* darstellbar ist, und folglich findet sich in dieser Classe Q eine Form (x^2, x', x''), welche offenbar

*) *D. A.* art. 287.

**) *Gauss: D. A.* art. 286.

durch Duplication der Form (x, x', xx'') entsteht; mithin ist $Q = K^2$, wo K die Classe bedeutet, welcher die Form (x, x', xx'') angehört. Das obige zu beweisende Theorem ist daher identisch mit dem folgenden:

Ist (A, B, C) eine Form des Hauptgeschlechtes der Determinante D, so ist die Gleichung

$$Az^2 + 2Bzy + Cy^2 = x^2$$

stets lösbar in ganzen Zahlen z, y, x, deren letzte relative Primzahl zu $2D$ ist.

§. 156.

Durch die vorstehende Betrachtung sind wir dahin geführt, die Lösbarkeit einer Gleichung von der Form

$$ax^2 + by^2 + cz^2 + 2a'yz + 2b'zx + 2c'xy = 0$$

in ganzen Zahlen x, y, z (oder was Dasselbe ist, die Lösbarkeit der allgemeinen Gleichung

$$au^2 + bv^2 + 2c'uv + 2b'u + 2a'v + c = 0$$

in *rationalen* Zahlen u, v) zu untersuchen. Dieselbe kann, allgemein zu reden, auf den speciellen Fall zurückgeführt werden, in welchem die Coefficienten a', b', $c' = 0$ sind*), und wir beschäftigen uns daher im Folgenden nur mit Gleichungen von der Form

$$ax^2 + by^2 + cz^2 = 0, \tag{1}$$

wo a, b, c drei gegebene, von Null verschiedene ganze Zahlen bedeuten, die wir ausserdem stets als *relative Primzahlen* annehmen, weil jeder andere Fall, wie man leicht erkennt, sich auf diesen zurückführen lässt**). Wir wollen nun eine Lösung x, y, z eine *eigentliche* Lösung nennen, wenn die drei Zahlen x, y, z *relative Primzahlen* sind; dann leuchtet ein, dass ax, by, cz ebenfalls relative Primzahlen sind; ginge nämlich eine Primzahl p in zweien von ihnen auf, so müsste p zufolge (1) auch in der dritten aufgehen; da aber höchstens einer der Coefficienten a, b, c durch p

*) *Gauss: D. A.* artt. 299, 300.

**) *Gauss: D. A.* art. 298.

theilbar sein kann, so wären wenigstens zwei der Zahlen x, y, z theilbar durch p, also keine relative Primzahlen.

Nach dieser Vorbemerkung beginnen wir unsere Untersuchung*), indem wir uns die folgende Aufgabe stellen:

I. *Aus einer gegebenen eigentlichen Lösung* $x = u$, $y = v$, $z = w$ *der Gleichung* (1) *ihre sämmtlichen Lösungen abzuleiten.*

Da au, bv, cw relative Primzahlen sind, und eine von ihnen, z. B. au, zufolge der Gleichung

$$au^2 + bv^2 + cw^2 = 0 \tag{2}$$

gerade ist, so haben auch die Zahlen $2au$, bv, cw keinen gemeinschaftlichen Theiler, und man kann daher (nach §. 24) die Gleichung

$$aul + bvm + cwn = 1$$

so lösen, dass l gerade, und folglich die eine der beiden Zahlen m, n gerade, die andere ungerade wird; setzt man nun

$$al^2 + bm^2 + cn^2 = h$$

und

$$u' = 2l - hu,\ v' = 2m - hv,\ w' = 2n - hw,$$

so wird h ungerade, und man erhält**)

$$au'^2 + bv'^2 + cw'^2 = 0 \tag{3}$$

$$auu' + bvv' + cww' = 2 \tag{4}$$

$$u \equiv u',\ v \equiv v',\ w \equiv w' \pmod{2}; \tag{5}$$

man kann daher

$$vw' - wv' = 2u'',\ wu' - uw' = 2v'',\ uv' - vu' = 2w'' \tag{6}$$

setzen, wo u'', v'', w'' ganze Zahlen bedeuten, welche mit den andern noch durch folgende Relationen***) verbunden sind:

---

*) Sie ist der Kürze halber synthetisch geführt; derselbe Gegenstand ist auf andere Weise behandelt in der mir erst nachträglich bekannt gewordenen Abhandlung von *G. Cantor: De aequationibus secundi gradus indeterminatis.* 1867.

**) Umgekehrt lässt sich aus (2), (3), (4), (5) leicht beweisen, dass a, b, c relative Primzahlen sind, und dass sowohl u, v, w, als auch u', v', w' eigentliche Lösungen der Gleichung (1) bilden; doch ist dies für unsere Zwecke nicht nöthig.

***) Man findet z. B. die erste der Gleichungen (7) aus der identischen Gleichung

$$(bv^2 + cw^2)(bv'^2 + cw'^2) = (bvv' + cww')^2 + bc(vw' - wv')^2$$

unter Berücksichtigung von (2), (3), (4), (6); die Gleichung (8) ergiebt sich

$$\left.\begin{aligned} auu' &= 1 + bcu''^2 \\ bvv' &= 1 + cav''^2 \\ cww' &= 1 + abw''^2 \end{aligned}\right\} \tag{7}$$

$$bcu''^2 + cav''^2 + abw''^2 = -1 \tag{8}$$

$$\left.\begin{aligned} vw' + wv' &= 2av''w'' \\ wu' + uw' &= 2bw''u'' \\ uv' + vu' &= 2cu''v'' \end{aligned}\right\} \tag{9}$$

Mit Hülfe derselben ist es leicht, unsere Aufgabe allgemein zu lösen. Sind x, y, z drei beliebige ganze Zahlen, so werden auch

$$\left.\begin{aligned} t &= au'x + bv'y + cw'z \\ t' &= aux + bvy + cwz \\ t'' &= u''x + v''y + w''z \end{aligned}\right\} \tag{10}$$

ganze Zahlen, welche zufolge (5) der Bedingung

$$t \equiv t' \pmod{2} \tag{11}$$

genügen; umgekehrt, sind t, t', t'' drei beliebige ganze Zahlen, welche nur der Bedingung (11) unterworfen sind, so folgt aus (10) unter Berücksichtigung von (5), (7) und (9), dass

$$\left.\begin{aligned} 2x &= ut + u't' - 2bcu''t'' \\ 2y &= vt + v't' - 2cav''t'' \\ 2z &= wt + w't' - 2abw''t'' \end{aligned}\right\} \tag{12}$$

gerade, also x, y, z ganze Zahlen sind. Multiplicirt man diese letzten Gleichungen resp. mit ax, by, cz, und addirt mit Rücksicht auf (10), so folgt

$$ax^2 + by^2 + cz^2 = tt' - abct''^2;$$

mithin haben wir folgendes Resultat: *Bilden die ganzen Zahlen x, y, z eine Lösung der Gleichung* (1), *so werden t, t', t'' vermöge* (10) *ganze Zahlen, welche den Bedingungen* (11) *und*

$$tt' = abct''^2 \tag{13}$$

genügen; umgekehrt, befriedigen die ganzen Zahlen t, t', t'' die Be-

---

durch Addition aus (7) mit Rücksicht auf (4); und die erste der Gleichungen (9) folgt aus der Identität

$$(auu' + bvv' + cww')(vw' + wv') - a(wu' - uw')(uv' - vu')$$
$$= (au^2 + bv^2 + cw^2)v'w' + (au'^2 + bv'^2 + cw'^2)vw.$$

dingungen (11) *und* (13), *so werden* x, y, z *vermöge* (12) *ganze Zahlen, welche der Gleichung* (1) *genügen**).

Zur Vervollständigung fügen wir hinzu: *Damit die Zahlen* x, y, z *eine eigentliche Lösung der Gleichung* (1) *bilden, ist ferner erforderlich und hinreichend, dass die Zahlen* t, t' *keinen ungeraden gemeinschaftlichen Theiler haben, und dass, wenn beide gerade sind,*

$$t + t' \equiv 2 \ (mod.\ 4) \tag{14}$$

ist.

Für unsern Zweck genügt es zu beweisen, dass die beiden angegebenen Bedingungen hinreichend sind. Gesetzt, es ginge eine Primzahl p in zweien der Zahlen ax, by, cz auf, so müsste sie zufolge (1) auch in der dritten aufgehen, mithin zufolge (10) auch in t und t'; da aber t, t' der Annahme nach keinen ungeraden gemeinschaftlichen Theiler haben, so müsste $p = 2$ sein, und es wären also t, t', ax, by, cz gerade Zahlen; dann würde aber aus (10) mit Rücksicht auf (5) folgen, dass $t + t' \equiv 0$ (mod. 4) wäre, während wir doch angenommen haben, dass $t + t' \equiv 2$ (mod. 4) ist, sobald t und t' gerade Zahlen sind. Hieraus folgt also, dass ax, by, cz relative Primzahlen sind, was zu beweisen war**).

---

*) Die allgemeinste Lösung der Gleichung (13), deren wir zwar in der Folge nicht bedürfen, besteht, wie man sehr leicht findet, in den Gleichungen

$$t = \tau d \omega^2, \quad t' = \tau d' \omega'^2, \quad t'' = \tau \omega \omega',$$

wo $d, d', \tau, \omega, \omega'$ beliebige ganze Zahlen bedeuten, welche der einzigen Bedingung

$$dd' = abc$$

unterworfen sind; man kann aber auch, ohne die Allgemeinheit zu beeinträchtigen, annehmen, dass τ der grösste gemeinschaftliche Theiler von t, t', t'', und dass τd, $\tau d'$ die grössten Theiler sind, welche τabc resp. mit t, t' gemeinschaftlich hat. Führt man diese Ausdrücke in (12) ein, so erhält man die binären quadratischen Formen

$$\frac{2x}{\tau} = (du, -bcu'', d'u'), \quad \frac{2y}{\tau} = (dv, -cav'', d'v'),$$
$$\frac{2z}{\tau} = (dw, -abw'', d'w'),$$

deren Variabeln ω, ω', und deren Determinanten zufolge (7) die Zahlen $-bc$, $-ca$, $-ab$ sind. Transformirt man diejenige dieser Formen, deren Determinante negativ ist, in eine reducirte Form (§. 64), so erhält man die einfachsten Lösungen.

**) Es ist leicht, wenn auch für unsern Zweck nicht erforderlich, die beiden angegebenen Bedingungen auf die Zahlen $d, d', \tau, \omega, \omega'$ zu übertragen: die Zahlen d, d' müssen relative Primzahlen sein, und nur, wenn

II. Bilden die Zahlen x, y, z eine eigentliche Lösung der Gleichung (1), so sind ax, by, cz relative Primzahlen, und man kann folglich drei Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ bestimmen, welche den Congruenzen

$$\mathfrak{A}z \equiv by \text{ (mod. } a), \quad \mathfrak{B}x \equiv cz \text{ (mod. } b), \quad \mathfrak{C}y \equiv ax \text{ (mod. } c) \qquad (15)$$

genügen, woraus in Verbindung mit (1)

$$\mathfrak{A}^2 \equiv -bc \text{ (mod. } a), \quad \mathfrak{B}^2 \equiv -ca \text{ (mod. } b), \quad \mathfrak{C}^2 \equiv -ab \text{ (mod. } c) \qquad (16)$$

folgt. Wir haben mithin folgenden Satz erhalten:

Ist die Gleichung (1) *eigentlich lösbar, so sind die Zahlen* $-bc$, $-ca$, $-ab$ *resp. quadratische Reste der Zahlen* a, b, c, *und jede eigentliche Lösung* x, y, z *führt durch die Congruenzen* (15) *zu drei völlig bestimmten Zahlclassen* $\mathfrak{A}$ (*mod.* a), $\mathfrak{B}$ (*mod.* b), $\mathfrak{C}$ (*mod.* c), *welche den Congruenzen* (16) *genügen**).

Von der grössten Wichtigkeit für unsere Untersuchungen ist es aber, dass dieser Satz sich in folgender Weise umkehren lässt:

Ist die Gleichung (1) *eigentlich lösbar, und sind drei Zahlen* $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ *gegeben, welche den Congruenzen* (16) *genügen, so kann man stets eigentliche Lösungen* x, y, z *finden, welche die Bedingungen* (15) *erfüllen.*

Um dies zu beweisen, bestimmen wir zunächst drei Zahlen X, Y, Z durch die (nach §. 25) stets vereinbaren Congruenzpaare

$$\left.\begin{array}{lll} X \equiv c \text{ (mod. } b), & Y \equiv a \text{ (mod. } c), & Z \equiv b \text{ (mod. } a) \\ X \equiv \mathfrak{C} \text{ (mod. } c), & Y \equiv \mathfrak{A} \text{ (mod. } a), & Z \equiv \mathfrak{B} \text{ (mod. } b) \end{array}\right\} \qquad (17)$$

aus welchen unter Berücksichtigung der Annahme (16) die der Gleichung (1) ähnliche Congruenz

$$aX^2 + bY^2 + cZ^2 \equiv 0 \text{ (mod. } abc) \qquad (1')$$

folgt, weil ihre linke Seite durch jede der drei relativen Primzahlen a, b, c theilbar ist. Da ferner die Existenz einer eigentlichen Lö-

$abc \equiv 0$ (mod. 8), können sie auch den grössten gemeinschaftlichen Theiler 2 haben; umgekehrt, genügt die Zerlegung $abc = dd'$ diesen Bedingungen, so kann man τ, ω, ω' so wählen, dass x, y, z eine eigentliche Lösung der Gleichung (1) bilden.

*) Wirft man zwei eigentliche Lösungen in dieselbe oder in verschiedene *Classen*, je nachdem sie zu denselben drei Zahlclassen $\mathfrak{A}$ (mod. a), $\mathfrak{B}$ (mod. b), $\mathfrak{C}$ (mod. c) führen oder nicht, so ist die Anzahl aller verschiedenen Classen *höchstens* gleich der Anzahl der incongruenten Wurzeln der Congruenz $x^2 \equiv 1$ (mod. abc), und der nachfolgende Satz behauptet die wirkliche Existenz aller dieser Classen von eigentlichen Lösungen.

sung u, v, w der Gleichung (1) angenommen ist, so behalten wir alle früheren Bezeichnungen bei und setzen

$$\left.\begin{aligned} T &\equiv au'X + bv'Y + cw'Z \\ T' &\equiv auX + bvY + cwZ \end{aligned}\right\} \pmod{2abc}, \qquad (10')$$

woraus zufolge (5)

$$T \equiv T' \pmod{2} \qquad (11')$$

und mit Rücksicht auf (7) und (9)

$$\left.\begin{aligned} 2X &\equiv uT + u'T' \pmod{2bc} \\ 2Y &\equiv vT + v'T' \pmod{2ca} \\ 2Z &\equiv wT + w'T' \pmod{2ab} \end{aligned}\right\} \qquad (12')$$

folgt; multiplicirt man diese Congruenzen resp. mit aX, bY, cZ, wodurch sie in Congruenzen nach dem Modulus $2abc$ übergehen, so ergiebt sich durch Addition unter Berücksichtigung von (1') und (10')

$$TT' \equiv 0 \pmod{abc}. \qquad (13')$$

Wir behaupten nun, dass die drei Zahlen T, T', abc keinen ungeraden gemeinschaftlichen Divisor haben, und dass, wenn abc gerade ist,

$$T + T' \equiv 2 \pmod{4} \qquad (14')$$

ist. Ginge nämlich eine ungerade Primzahl p in T, T' und abc, also auch z. B. in c auf, so würde Y zufolge (12') durch p theilbar sein, und da $a \equiv Y \pmod{c}$ ist, so hätten a und c den gemeinschaftlichen Theiler p, was unmöglich ist. Wenn ferner abc, und also auch z. B. c gerade ist, so sind zufolge (11') und (13') auch T und T' gerade Zahlen; wäre nun die Congruenz (14') unrichtig, so wäre $T' \equiv T \pmod{4}$, und aus (12') würde folgen, dass $2Y \equiv (v + v')T \equiv 0 \pmod{4}$, also Y gerade wäre, was abermals gegen die Congruenz $a \equiv Y \pmod{c}$ streitet, weil a relative Primzahl zu c ist.

Nach diesen Vorbereitungen sind wir im Stande, eine eigentliche Lösung x, y, z nachzuweisen, welche den Bedingungen (15) genügt; diese letztern gehen vermöge der Definition (17) der Zahlen X, Y, Z in die folgenden über

$$Yz \equiv Zy \pmod{a}, \quad Zx \equiv Xz \pmod{b}, \quad Xy \equiv Yx \pmod{c};$$

da ferner aus den Definitionen (10) und (10') der Zahlen t, t' T, T' die Congruenz

$$\left.\begin{array}{c} T't - Tt' \equiv \\ 2bcu''(Yz - Zy) + 2cav''(Zx - Xz) + 2abw''(Xy - Yx) \end{array}\right\} (\mathrm{mod.}\, 2abc)$$

folgt, und da u'', v'', w'' zufolge (7) resp. relative Primzahlen zu a, b, c sind, so fallen die von x, y, z zu erfüllenden Bedingungen (15) durchaus mit der einzigen Forderung

$$T't \equiv Tt' \ (\mathrm{mod.}\ 2abc)$$

zusammen, welcher die Zahlen t, t' genügen müssen; sollen ferner die Zahlen x, y, z eine eigentliche Lösung der Gleichung (1) bilden, so haben t und t' ausserdem noch die früher erwähnten Bedingungen (11), (13), (14) zu erfüllen. Dies Alles lässt sich in der That auf folgende Weise erreichen.

Ist abc ungerade, so sei d der grösste gemeinschaftliche Theiler der beiden Zahlen T und $abc = dd'$; da nun zufolge (13') TT' durch abc theilbar ist, so geht d' in T' auf, und da, wie oben gezeigt ist, die Zahlen T, T', abc keinen ungeraden gemeinschaftlichen Theiler haben, so sind d und d' relative Primzahlen, und d' ist zugleich der grösste gemeinschaftliche Theiler der beiden Zahlen T' und abc. Dann leuchtet ein, dass man allen Forderungen genügt, wenn man z. B. $t = d$, $t' = d'$, $t'' = 1$ nimmt; denn weil $t \equiv t' \equiv 1$ (mod. 2), so werden x, y, z ganze Zahlen, die wegen $tt' = abct''^2$ eine Lösung der Gleichung (1) bilden; diese Lösung ist eine eigentliche, weil t, t' ungerade relative Primzahlen sind; da endlich $t \equiv t'$, $T \equiv T'$ (mod. 2), und $T't \equiv Tt' \equiv 0$ (mod. dd') ist, so folgt auch $T't \equiv Tt'$ (mod. $2abc$) d. h. die eigentliche Lösung x, y, z genügt den vorgeschriebenen Congruenzen (15).

Ist aber abc, und folglich auch T, T' gerade, und zwar $T + T' \equiv 2$ (mod. 4), so können wir der Symmetrie wegen annehmen, es sei $T \equiv 0$, $T' \equiv 2$ (mod. 4); dann sei d wieder der grösste gemeinschaftliche Theiler der beiden Zahlen T und $abc = dd'$, so wird d' in T' aufgehen. Ist nun d' ungerade, so genügt man allen Bedingungen, wenn man z. B. $t = 2d$, $t' = 2d'$, $t'' = 2$ nimmt; denn es ist $t \equiv 0$, $t' \equiv 2$ (mod. 4), $tt' = abct''^2$, $T't \equiv Tt' \equiv 0$ (mod. $2abc$), und t, t' haben keinen ungeraden gemeinschaftlichen Theiler. Ist aber d' gerade, so kann man wieder durch $t = d$, $t' = d'$, $t'' = 1$ allen Bedingungen genügen; da nämlich $T:d$ relative Primzahl zu d' und folglich ungerade ist, so muss, weil $T \equiv 0$ (mod. 4), auch $d \equiv 0$ (mod. 4) sein; da ferner d' in T' aufgeht, und $T' \equiv 2$ (mod. 4) ist, so muss auch $d' \equiv 2$ (mod. 4) sein; mithin ist $t \equiv 0$, $t' \equiv 2$ (mod. 4); es ist ferner $tt' = abct''^2$, und

die Zahlen t, t' haben keinen ungeraden gemeinschaftlichen Theiler; da endlich die Quotienten $T:d$ und $T':d'$ ungerade sind, so ist ihre Differenz gerade, und folglich, wenn man mit $dd' = abc$ multiplicirt, $Td' - T'd = Tt' - T't \equiv 0 \pmod{2\,abc}$, was zu beweisen war.

Es hat keine Schwierigkeit, ausser den eben angegebenen speciellen Lösungen, welche die vorgeschriebenen Congruenzen (15) erfüllen, alle andern zu bestimmen, und man findet namentlich leicht, dass zwei eigentliche Lösungen x, y, z und x_1, y_1, z_1, welche resp. durch die Werthe t, t', t'' und t_1, t_1', t_1'' hervorgebracht werden, stets und nur dann denselben Congruenzen (15) genügen, wenn $tt_1' \equiv t't_1 \pmod{2\,abc}$ ist*); allein alle diese an sich interessanten Vervollständigungen sind für unsere Zwecke nicht erforderlich. Wir begnügen uns daher, aus den obigen Resultaten noch den Beweis des folgenden Satzes abzuleiten, dessen wir später durchaus bedürfen.

III. *Ist die Gleichung* (1) *eigentlich lösbar, und ist* $-bc$ *quadratischer Rest von* ap^2, *wo* p *eine in* bc *nicht aufgehende Primzahl bedeutet, so besitzt die Gleichung* (1) *auch solche eigentliche Lösungen* x, y, z, *welche der Bedingung* $x \equiv 0 \pmod{p}$ *genügen.*

Der Annahme zufolge besitzt die Gleichung (1) eine eigentliche Lösung u, v, w, und wir können alle hieraus in I. gezogenen Folgerungen für uns in Anspruch nehmen; es versteht sich von selbst, dass wir den vorstehenden Satz nur für den Fall zu beweisen brauchen, dass keine der beiden Zahlen u, u' durch p theilbar ist.

Ist nun p ungerade, so kann man, da der Annahme nach $-bc \equiv \alpha^2 \pmod{p}$ ist, das Vorzeichen von α so wählen, dass $bcu'' + \alpha$ nicht theilbar durch p ist; wären nämlich beide Zahlen

*) Hieraus folgt, dass allen zu derselben Classe gehörigen eigentlichen Lösungen dieselbe Zerlegung $abc = dd'$ entspricht, mit einziger Ausnahme des Falles, wo $abc \equiv 2 \pmod{4}$, in welchem der Factor 2 nach Belieben in d oder in d' aufgenommen werden kann, ohne dass eine Aenderung der Classe eintritt. Auf diese Weise ergiebt sich (vergl. die früheren Noten), dass die Anzahl der wesentlich verschiedenen Zerlegungen, und also auch die der wirklich existirenden Classen genau mit der Anzahl der incongruenten Wurzeln der Congruenz $x^2 \equiv 1 \pmod{abc}$ übereinstimmt; hierin liegt also ein neuer Beweis des obigen Satzes. Aber es schien angemessener, ihn so zu führen, dass zugleich eine Lösung gefunden wird, welche den vorgeschriebenen Congruenzen genügt.

$bcu'' + \alpha$ und $bcu'' - \alpha$ durch p theilbar, so müsste auch ihre Differenz 2α, also auch α durch die ungerade Primzahl p theilbar sein, was gegen $-bc \equiv \alpha^2 \pmod{p}$ und die Annahme streitet, dass p nicht in bc aufgeht. Da nun u ebenfalls nicht durch p theilbar ist, so kann man eine Zahl ω stets so bestimmen (§. 25), dass sie der Congruenz

$$u\omega \equiv bcu'' + \alpha \pmod{p}$$

genügt und ausserdem relative Primzahl zu $2abc$ wird, weil ω, falls p in $2abc$, also in a aufgehen sollte, schon vermöge dieser Congruenz relative Primzahl zu p wird. Setzt man nun

$$t = \tau\omega^2, \quad t' = \tau abc, \quad t'' = \tau\omega,$$

wo $\tau = 1$ oder $= 2$ zu nehmen ist, je nachdem abc ungerade oder gerade ist, so erhält man eine entsprechende eigentliche Lösung x, y, z, welche auch der Bedingung $x \equiv 0 \pmod{p}$ genügt. Ist nämlich abc ungerade, also $\tau = 1$, so ist $t \equiv t' \equiv 1 \pmod{2}$; ist aber abc gerade, also $\tau = 2$, so ist $t \equiv 2$, $t' \equiv 0 \pmod{4}$; da ferner ω relative Primzahl zu abc ist, so haben t, t' keinen ungeraden gemeinschaftlichen Divisor, und da $tt' = abct''^2$ ist, so bilden x, y, z eine eigentliche Lösung der Gleichung (1). Nun ist nach (12)

$$\begin{aligned} 2x &= ut + u't' - 2bcu''t'' \\ &= \tau(u\omega^2 - 2bcu''\omega + abcu') \end{aligned}$$

also mit Rücksicht auf (7)

$$2ux = \tau\,\{(u\omega - bcu'')^2 + bc\} \equiv 0 \pmod{p},$$

weil $u\omega - bcu'' \equiv \alpha$, $bc \equiv -\alpha^2$ ist; da endlich $2u$ nicht durch p theilbar ist, so folgt hieraus $x \equiv 0 \pmod{p}$.

Wir gehen jetzt zu dem Falle $p = 2$ über. Ist erstens a gerade, aber nicht $\equiv 0 \pmod{8}$, so ergiebt sich leicht, da der Annahme nach $-bc$ quadratischer Rest von $4a$, also $bc \equiv -1 \pmod{8}$ ist, dass u gar nicht ungerade sein kann; da nämlich a gerade, also bv, cw ungerade sind, und $b \equiv -c \pmod{8}$ ist, so folgt aus $au^2 + bv^2 + cw^2 = 0$, dass $au^2 \equiv 0 \pmod{8}$, und folglich, da a nicht $\equiv 0 \pmod{8}$ ist, jedenfalls u gerade sein muss; und offenbar haben dann alle anderen eigentlichen Auflösungen x, y, z dieselbe Eigenschaft $x \equiv 0 \pmod{2}$. Ist zweitens $a \equiv 0 \pmod{8}$, also $-bc \equiv 1 \pmod{8}$, so nehme man $t'' = 1$, und $tt' = abc$ der Art, dass einer der beiden Factoren, z. B. $t \equiv 2 \pmod{4}$, also der andere $t' \equiv 0 \pmod{4}$ wird, und dass sie keinen ungeraden gemeinschaftlichen Divisor erhalten, was sich stets erreichen lässt.

Hieraus folgt, dass die Zahlen x, y, z eine eigentliche Lösung bilden werden. Da nun der Voraussetzung nach u ungerade ist, und da aus $1 + bcu''^2 = auu' \equiv 0$ (mod. 8) folgt, dass auch u'' ungerade ist, so ergiebt sich

$$2x = ut + u't' - 2bcu''t'' \equiv 2 + 0 - 2 \equiv 0 \text{ (mod. 4)},$$

also ist $x \equiv 0$ (mod. 2). Ist endlich drittens a ungerade, und $-bc$ quadratischer Rest von $4a$, also $bc \equiv -1$ (mod. 4), so nehme man $t'' = 1$, und nach Belieben $tt' = abc$, nur so, dass t und t' relative Primzahlen werden; dann bilden x, y, z eine eigentliche Lösung, weil ausserdem $t \equiv t' \equiv 1$ (mod. 2) ist. Da nun der Voraussetzung nach keine der Zahlen u, u' gerade ist, so folgt aus $auu' = 1 + bcu''^2$, dass u'' gerade, und folglich $auu' \equiv 1$ (mod. 4) ist; mithin ist $ut.u't' = auu'.bc \equiv -1$ (mod. 4), also $ut \equiv -u't'$ (mod. 4), und hieraus ergiebt sich

$$2x = ut + u't' - 2bcu''t'' \equiv 0 \text{ (mod. 4)},$$

also ist $x \equiv 0$ (mod. 2).

Hiermit ist der obige Satz vollständig bewiesen, und dieser Beweis enthält offenbar eine Methode, aus einer eigentlichen Lösung u, v, w einer Gleichung, deren Coefficienten a, b, c sind, eine eigentliche Lösung $x:p$, y, z derjenigen Gleichung abzuleiten, deren Coefficienten ap^2, b, c sind, vorausgesetzt, dass $-bc$ quadratischer Rest von ap^2 und nicht durch die Primzahl p theilbar ist. Durch wiederholte Anwendung desselben Satzes gelangt man offenbar zu folgendem Resultat:

Sind die Zahlen $A = aP^2$, $B = bQ^2$, $C = cR^2$ relative Primzahlen, und sind die Zahlen $-BC$, $-CA$, $-AB$ resp. quadratische Reste von A, B, C, so folgt aus der Existenz einer eigentlichen Lösung der Gleichung

$$ax^2 + by^2 + cz^2 = 0$$

stets die Existenz einer eigentlichen Lösung der Gleichung

$$Ax^2 + By^2 + Cz^2 = 0.$$

§. 157.

Durch den zuletzt bewiesenen Satz ist offenbar die Frage nach der eigentlichen Lösbarkeit der Gleichung

$$ax^2 + by^2 + cz^2 = 0 \quad (1)$$

auf den Fall zurückgeführt, in welchem keine der relativen Primzahlen a, b, c durch ein Quadrat theilbar ist; als eine erforderliche Bedingung für die Lösbarkeit ist ferner im vorigen Paragraphen (II) erkannt, dass die Zahlen $-bc$, $-ca$, $-ab$ resp. quadratische Reste von den Zahlen a, b, c sein müssen, und ausserdem leuchtet ein, dass die letzteren unmöglich alle dasselbe Vorzeichen haben können. Mit Hülfe einer Reductionsmethode, welche im Wesentlichen von *Lagrange**) herrührt, lässt sich nun wirklich beweisen, dass diese Bedingungen auch die hinreichenden sind, dass also folgender Satz**) besteht:

Sind a, b, c drei von Null verschiedene und durch kein Quadrat theilbare relative Primzahlen, welche nicht alle dasselbe Vorzeichen haben, und sind die Zahlen $-bc$, $-ca$, $-ab$ resp. quadratische Reste der Zahlen a, b, c; so ist die Gleichung (1) *eigentlich lösbar.*

Zunächst bemerken wir, dass der Satz in dem speciellen Falle richtig ist, wenn einer der Coefficienten, z. B. $a = +1$, ein anderer, z. B. $b = -1$ ist; denn man genügt der Gleichung (1) durch die relativen Primzahlen $x = y = 1$, $z = 0$.

Um uns nun bequemer ausdrücken zu können, nennen wir, indem wir den absoluten Werth einer Grösse k mit (k) bezeichnen, dasjenige der drei Producte (bc), (ca), (ab), welches der Grösse nach zwischen den beiden anderen liegt, den *Index* der Gleichung (1), und wenn etwa zwei dieser Producte oder alle drei einander gleich sein sollten, so soll unter dem Index der gemeinschaftliche

*) *Sur la solution des problèmes indéterminés du second degré.* Mém. de l'Acad. de Berlin. T. XXIII. 1769. (Œuvres de L. T. II. 1868. p. 375.) — *Additions aux Élémens d'Algèbre par L. Euler.* §. V.

**) *Legendre: Théorie des Nombres*, 3me éd. T. I. §§. III, IV. — *Gauss: D. A.* artt. 294, 295. — Der nachfolgende Beweis lässt sich auf den Fall ausdehnen, dass a, b, c quadratische Divisoren besitzen.

Werth dieser beiden oder aller Producte verstanden werden. Aus dieser Erklärung ergiebt sich unmittelbar die Richtigkeit des Satzes für den Fall, dass ihr Index $= 1$ ist; denn dann muss, wie man leicht erkennt, $(a) = (b) = (c) = 1$ sein, und da die Coefficienten nicht alle dasselbe Vorzeichen haben, so ergiebt sich die Lösbarkeit der Gleichung aus der vorausgeschickten Bemerkung.

Um nun den Beweis allgemein zu führen, nehmen wir an, er sei schon geleistet für alle Gleichungen, deren Index kleiner als eine bestimmte positive ganze Zahl J ist, und zeigen, dass der Satz dann auch für alle Gleichungen gelten muss, deren Index $= J$ ist. Gelingt dies, so gilt der Satz allgemein, weil er für $J = 1$ richtig ist.

Es sei daher $J \geqq 2$ der Index der Gleichung (1). Nehmen wir an, was der Symmetrie wegen erlaubt ist, es sei $(a) \leqq (b) \leqq (c)$, also auch $(ab) \leqq (ac) \leqq (bc)$, so ist $J = (ac)$; wäre nun $(b) = (c)$, so müsste, weil b und c relative Primzahlen sind, $(b) = (c) = 1$ sein, woraus auch $J = 1$ folgen würde, was mit unserer Annahme streitet; mithin ist

$$(a) \leqq (b) < (c),\ (ab) < (ac) = J \leqq (bc). \tag{2}$$

Der Annahme nach ist nun $-ab$ quadratischer Rest von c, und folglich kann man eine Zahl r so bestimmen, dass $ar^2 \equiv -b$ (mod. c), und zugleich $(r) \leqq \frac{1}{2}(c)$ wird; setzt man dann

$$ar^2 + b = cC, \tag{3}$$

so wird C eine ganze Zahl, deren absoluter Werth

$$(C) \leqq \frac{(a)r^2 + (b)}{(c)} < \tfrac{1}{4}J + 1 < J \tag{4}$$

ist, weil $(r) \leqq \frac{1}{2}(c)$, $(ac) = J \geqq 2$, und $(b) < (c)$ ist.

Ist nun $C = 0$, so folgt $b = -ar^2$, also, da b relative Primzahl zu a und durch kein Quadrat theilbar ist, $(r) = 1$ und $b = -a = \pm 1$, und mithin besitzt die Gleichung (1) in diesem Fall wieder die eigentliche Lösung $x = y = 1$, $z = 0$.

Ist aber C von Null verschieden, so führen wir die Gleichung (1) folgendermaassen auf eine andere von kleinerem Index zurück. Es sei a' der grösste gemeinschaftliche Divisor der drei in der Gleichung (3) vorkommenden Glieder ar^2, b, cC, so ist a' zugleich der grösste gemeinschaftliche Divisor von je zweien dieser Zahlen, so dass die drei Glieder der Gleichung

$$\frac{ar^2}{a'} + \frac{b}{a'} = \frac{cC}{a'}$$

gewiss relative Primzahlen sind. Da nun a' in b aufgeht, also relative Primzahl zu c und zu a ist, so muss a' in C und in r^2, also auch in r selbst aufgehen, weil a' als Divisor von b durch kein Quadrat theilbar ist. Man kann daher

$$r = a'\alpha, \quad b = a'\beta, \quad C = a'C' = a'c'\gamma^2 \tag{5}$$

setzen, wo γ^2 das grösste in $C' = c'\gamma^2$ aufgehende Quadrat bedeutet; hierdurch geht die Gleichung (3) in die folgende über

$$aa'\alpha^2 + \beta = cc'\gamma^2, \tag{6}$$

deren drei Glieder also relative Primzahlen sind; setzen wir endlich noch

$$b' = a\beta, \tag{7}$$

so sind hierdurch drei Zahlen a', b', c' definirt, welche, wie wir beweisen wollen, dieselben Eigenschaften besitzen, wie die gegebenen Zahlen a, b, c.

Dass erstens keine der Zahlen a', b', $c' = 0$ ist, leuchtet ein, weil $a'b' = a'a\beta = ab$ ist, und c' in C aufgeht. Aus $a'b' = ab$ folgt ferner, dass a', b' relative Primzahlen und durch kein Quadrat theilbar sind, weil a, b dieselben Eigenschaften haben; da ferner γ^2 das grösste in $C' = c'\gamma^2$ aufgehende Quadrat ist, so kann c' durch kein Quadrat theilbar sein; und da die Glieder der Gleichung (6) relative Primzahlen sind, so ist c' auch relative Primzahl zu $aa'\beta = a'b'$.

Die Zahlen a', b', c' können auch nicht alle dasselbe Vorzeichen haben; ist nämlich $ab = a'b'$ negativ, so haben a', b' entgegengesetzte Zeichen; ist aber ab positiv, folglich ca und bc negativ, so ergiebt sich aus der Gleichung $ar^2 + b = ca'c'\gamma^2$, dass $a'c'$ negativ ist, dass also a', c' entgegengesetzte Vorzeichen haben.

Da ferner zufolge der Gleichung (6), deren drei Glieder relative Primzahlen sind, die drei Zahlen $\beta cc'$, $aca'c'$, $-aa'\beta = -a'b'$ resp. quadratische Reste der drei Zahlen aa', β, c' sein müssen, und da nach Voraussetzung die beiden Zahlen $-bc = -\beta a'c$, $-ca$ resp. Reste von den beiden Zahlen a, $b = a'\beta$ sind, so ergiebt sich hieraus leicht, dass die drei Zahlen $-b'c'$, $-c'a'$, $-a'b'$ resp. Reste der drei Zahlen a', b', c' sind.

Endlich ist $(a'b') = (ab) < J$ zufolge (2), und $(c'a') \leqq (c'a')\gamma^2 = (C) < J$ zufolge (4); mithin ist der Index der Gleichung

$$a'x'^2 + b'y'^2 + c'z'^2 = 0$$

gewiss kleiner als J, und folglich ist sie nach unserer obigen Voraussetzung lösbar in relativen Primzahlen x', y', z'; da nun die Zahlen $a'\alpha x' - \beta y'$, $x' + a\alpha y'$ nicht beide verschwinden, weil sonst auch $x' = y' = 0$ wäre, so kann man

$$mx = a'\alpha x' - \beta y'; \quad my = x' + a\alpha y'; \quad mz = c'\gamma z'$$

setzen, wo m den grössten gemeinschaftlichen Theiler der drei Zahlen rechter Hand bedeutet; hieraus folgt aber mit Beachtung von (5), (6), (7)

$$m^2(ax^2 + by^2 + cz^2) = cc'\gamma^2(a'x'^2 + b'y'^2 + c'z'^2) = 0,$$

also, da m nicht $= 0$ ist, auch

$$ax^2 + by^2 + cz^2 = 0;$$

da endlich die Zahlen x, y, z keinen gemeinschaftlichen Theiler haben, und keine der Zahlen a, b, c durch ein Quadrat theilbar ist, so sind x, y, z auch relative Primzahlen und bilden folglich eine eigentliche Lösung der Gleichung (1).

Hiermit ist der Schluss vollständig durchgeführt, und also auch der obige Satz allgemein bewiesen. Es leuchtet ferner ein, dass in der successiven Zurückführung der Gleichung (1) auf ähnliche Gleichungen von immer kleinerem Index und endlich auf eine Gleichung, in welcher ein Coefficient $= +1$, ein anderer $= -1$ ist, auch eine Methode liegt, eine Lösung derselben zu finden.

Nachdem für diejenigen Gleichungen, deren Coefficienten durch kein Quadrat theilbar sind, die oben genannten *erforderlichen* Bedingungen zugleich als *hinreichend* für die Existenz eigentlicher Lösungen erkannt sind, so geht aus dem Schlusssatze des vorigen Paragraphen hervor, dass genau Dasselbe Statt findet für alle Gleichungen (1), deren Coefficienten von Null verschieden und relative Primzahlen sind. Wir können daher das Gesammtresultat unserer Untersuchungen in dem folgenden wichtigen Satze niederlegen:

Sind die Zahlen a, b, c relative Primzahlen und von Null verschieden, so ist die Gleichung

$$ax^2 + by^2 + cz^2 = 0$$

stets und nur dann in relativen Primzahlen x, y, z lösbar, wenn die Zahlen $-bc$, $-ca$, $-ab$ resp. quadratische Reste von den Zahlen a, b, c sind, und diese letztern nicht alle dasselbe Vorzeichen haben; ist ferner

$-bc \equiv \mathfrak{A}^2$ *(mod. a)*, $-ca \equiv \mathfrak{B}^2$ *(mod. b)*, $-ab \equiv \mathfrak{C}^2$ *(mod. c)*, *so ist die obige Gleichung in relativen Primzahlen* x, y, z *der Art lösbar, dass*

$$\mathfrak{A}z \equiv by \text{ (mod. } a), \ \mathfrak{B}x \equiv cz \text{ (mod. } b), \ \mathfrak{C}y \equiv ax \text{ (mod. } c)$$

wird.

§. 158.

Mit Hülfe dieses Satzes lässt sich nun das oben (§. 155) erwähnte grosse Theorem von *Gauss* leicht beweisen:

Jede Classe des Hauptgeschlechtes entsteht durch Duplication.

Als Repräsentanten der dem Hauptgeschlechte der Determinante D angehörenden Classe wählen wir eine Form (A, B, C), deren erster Coefficient A relative Primzahl zu $2D$ ist (§. 93). Da die Zahl A durch diese Form darstellbar ist, und alle Einzel-Charaktere derselben den Werth $+1$ haben, so ist A quadratischer Rest von jeder in D aufgehenden ungeraden Primzahl, und auch von 4 oder von 8, falls D durch 4 oder 8 theilbar ist (§. 122); mithin ist (nach §. 37) A quadratischer Rest von D selbst (umgekehrt ergiebt sich leicht, zum Theil mit Hülfe des Reciprocitätssatzes, dass die Form (A, B, C) gewiss dem Hauptgeschlecht angehört, wenn A relative Primzahl zu $2D$, quadratischer Rest von D, und, falls D negativ sein sollte, positiv ist). Ja, man kann sogar voraussetzen, dass A quadratischer Rest von $4D$ ist, d. h. dass $A \equiv 1$ (mod. 4), oder $A \equiv 1$ (mod. 8) ist, je nachdem D ungerade oder gerade ist. Dies ist in der That von selbst der Fall, wenn $D \equiv 3$ (mod. 4), oder $D \equiv 0$ (mod. 8) ist; sollte ferner A in den übrigen Fällen dieser Bedingung nicht genügen, wäre also $A \equiv 3$ (mod. 4), $\equiv 7$ (mod. 8), $\equiv 3$ (mod. 8), $\equiv 5$ (mod. 8), je nachdem $D \equiv 1$ (mod. 4), $\equiv 2$ (mod. 8), $\equiv 6$ (mod. 8), $\equiv 4$ (mod. 8), so kann man die Form (A, B, C) durch eine Substitution $\binom{\alpha, -1}{1, \ \ 0}$ in eine Form transformiren, deren erster Coefficient $A' = A\alpha^2 + 2B\alpha + C$ relative Primzahl zu $2D$ ist und zugleich die verlangte Eigenschaft besitzt; da nämlich $AA' = (A\alpha + B)^2 - D$ ist, so braucht man α nur so zu wählen, dass $A\alpha + B$ im ersten Falle gerade, in den drei übrigen Fällen aber ungerade wird, was sich stets in der Art erreichen lässt, dass $A\alpha + B$ zugleich relative Primzahl zu D wird.

Wir setzen daher voraus, dass A quadratischer Rest von $4D$ und relative Primzahl zu $4D$ ist; da nun $4D \equiv (2B)^2$ (mod. A), also quadratischer Rest von A ist, und da die Zahlen A, $4D$ nicht beide negativ sind, so besitzt die Gleichung

$$Ax^2 + 4Dy^2 - z^2 = 0$$

immer eigentliche Lösungen x, y, z, welche der Bedingung

$$2Bz \equiv 4Dy, \quad \text{also} \quad z \equiv 2By \pmod{A}$$

genügen (§. 157); man kann daher $z = At + 2By$ setzen, wodurch die obige Gleichung in die folgende übergeht

$$At^2 + 2B(2y) + C(2y)^2 = x^2;$$

da Ax, $2Dy$, z relative Primzahlen sind, so sind auch t, $2y$ relative Primzahlen, und folglich ist (A, B, C) einer Form äquivalent (§. 60), deren erster Coefficient x^2 eine Quadratzahl und relative Primzahl zu $2D$ ist, und welche folglich (nach §. 155) durch Duplication einer Form entsteht, deren erster Coefficient $\pm x$ ist. Was zu beweisen war*).

Die unendlich vielen eigentlichen Lösungen x, y, z der obigen Gleichung, welche der Bedingung $z \equiv 2By$ (mod. A) genügen, zerfallen nun noch in verschiedene Classen in Bezug auf den Modul $4D$ (§. 156. II.); auf den Zusammenhang dieser Lösungen mit den verschiedenen Classen, durch deren Duplication dieselbe gegebene Classe des Hauptgeschlechtes entsteht, können wir aber hier nicht mehr eingehen.

§. 159.

Die Theorie der binären quadratischen Formen, ihrer Aequivalenz und Composition bildet nur einen speciellen Fall von der Theorie derjenigen homogenen Formen $n$ten Grades mit n Veränderlichen, welche sich in lineare Factoren mit algebraischen

*) Die Zurückführung dieses Satzes von *Gauss* auf den von *Lagrange* und *Legendre* ist, wie ich jetzt nachträglich bemerke, zuerst von *Arndt* ausgeführt (*Ueber die Anzahl der Genera der quadratischen Formen;* Crelle's Journal LVI), doch weicht die obige Darstellung in mehreren Puncten von der seinigen ab. In Wahrheit gehört der Satz von *Lagrange* nach Inhalt und Methode des Beweises in die Theorie der ternären Formen. — Man vergl. ferner *Kronecker: Ueber den Gebrauch der Dirichlet'schen Methoden in der Theorie der quadratischen Formen* (Monatsber. d. Berliner Ak. 12. Mai 1864).

Coefficienten zerlegen lassen. Diese Formen sind zuerst von *Lagrange**) betrachtet; später hat *Dirichlet***) sich vielfach mit diesem Gegenstande beschäftigt, aber er hat von seinen weit gehenden Untersuchungen nur diejenige veröffentlicht, welche die Transformationen solcher Formen in sich selbst (vergl. §§. 61, 62) oder, was dasselbe ist, die Theorie der Einheiten für die entsprechenden algebraischen Zahlen behandelt; endlich hat *Kummer****) durch die Schöpfung der idealen Zahlen einen neuen Weg betreten, welcher nicht nur zu einer sehr bequemen Ausdrucksweise, sondern auch zu einer tieferen Einsicht in die wahre Natur der algebraischen Zahlen führt. Indem wir versuchen, den Leser in diese neuen Ideen einzuführen, stellen wir uns auf einen etwas höheren Standpunct und beginnen damit, einen Begriff einzuführen, welcher wohl geeignet scheint, als Grundlage für die höhere Algebra und die mit ihr zusammenhängenden Theile der Zahlentheorie zu dienen.

I. Unter einem *Körper* wollen wir jedes System von unendlich vielen reellen oder complexen Zahlen verstehen, welches in sich so abgeschlossen und vollständig ist, dass die Addition, Subtraction, Multiplication und Division von je zwei dieser Zahlen immer wieder eine Zahl desselben Systems hervorbringt. Der einfachste Körper wird durch alle rationalen, der grösste Körper durch alle Zahlen gebildet. Wir nennen einen Körper A einen *Divisor* des Körpers M, diesen ein *Multiplum* von jenem, wenn alle in A enthaltenen Zahlen sich auch in M vorfinden; man findet leicht, dass der Körper der rationalen Zahlen ein Divisor von jedem andern Körper ist. Der Inbegriff aller Zahlen, welche gleichzeitig in zwei Körpern A, B enthalten sind, bildet wieder einen Körper D, welcher der *grösste* gemeinschaftliche Divisor der beiden Körper A, B genannt werden kann, weil offenbar jeder gemeinschaftliche Divisor von A und B nothwendig ein Divisor von D ist; ebenso existirt immer ein Körper M, welcher das *kleinste* gemeinschaftliche Multiplum von A und B heissen soll, weil er ein Divisor von jedem andern gemeinschaftlichen Multiplum der beiden Körper ist. Entspricht ferner einer jeden Zahl a des Körpers A eine Zahl $b = \varphi(a)$

*) *Sur la solution des problèmes indéterminés du second degré.* §. VI. Mém. de l'Ac. de Berlin. T. XXIII, 1769. (Œuvres de L. T. II, 1868, p. 375.) — *Additions aux Élémens d'Algèbre par L. Euler.* §. IX.

**) Vergl. Anm. zu §. 141.

***) Vergl. Anm. zu §. 16.

in der Weise, dass $\varphi(a+a') = \varphi(a) + \varphi(a')$, und $\varphi(aa') = \varphi(a)\,\varphi(a')$ ist, so bilden die Zahlen b (falls sie nicht sämmtlich verschwinden) ebenfalls einen Körper $B = \varphi(A)$, welcher *mit* A *conjugirt* ist und durch die *Substitution* φ aus A hervorgeht; dann ist rückwärts auch $A = \psi(B)$ mit B conjugirt. Zwei mit einem dritten conjugirte Körper sind auch mit einander conjugirt, und jeder Körper ist mit sich selbst conjugirt. Correspondirende Zahlen in zwei conjugirten Körpern A und B, wie a und $b = \varphi(a)$, sollen *conjugirte Zahlen* heissen.

Die einfachsten Körper sind diejenigen, welche nur eine *endliche* Anzahl von Divisoren besitzen. Nennt man m bestimmte Zahlen $\alpha_1, \alpha_2 \ldots \alpha_m$ *von einander abhängig* oder *unabhängig*, je nachdem die Gleichung $x_1\alpha_1 + x_2\alpha_2 + \cdots + x_m\alpha_m = 0$ in rationalen Zahlen $x_1, x_2 \ldots x_m$, die nicht sämmtlich verschwinden, lösbar ist oder nicht, so findet man durch sehr einfache Betrachtungen, auf die wir aber hier nicht eingehen wollen, dass aus einem Körper Ω von der angegebenen Art*) nur eine *endliche* Anzahl n von unabhängigen Zahlen $\omega_1, \omega_2 \ldots \omega_n$ sich auswählen lässt, dass also jede Zahl ω des Körpers stets und nur auf eine einzige Art durch die Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n = \sum h_\iota\omega_\iota \tag{1}$$

darstellbar ist, wo $h_1, h_2 \ldots h_n$ *rationale Zahlen* bedeuten. Wir wollen die Zahl n den *Grad*, ferner den Complex der n unabhängigen Zahlen ω_ι eine *Basis des Körpers* Ω, und die n Zahlen h_ι die dieser Basis entsprechenden *Coordinaten der Zahl* ω nennen; offenbar bilden je n Zahlen von der Form (1) wieder eine solche Basis, wenn die aus den entsprechenden n^2 Coordinaten gebildete Determinante von Null verschieden ist; einer solchen *Transformation* der Basis durch eine lineare Substitution entspricht eine Transformation der Coordinaten durch die sogenannte *transponirte* Substitution.

Die Forderung, dass die Zahlen ω des Körpers Ω durch Addition und Subtraction sich reproduciren sollen, wird durch ihre gemeinsame Form (1) schon erfüllt; für die Reproduction durch Multiplication ist ferner erforderlich und hinreichend, dass jedes

*) Ersetzt man die rationalen Zahlen überall durch Zahlen eines Körpers R, so gelten die nachfolgenden Betrachtungen auch für einen Körper Ω, welcher nur eine endliche Anzahl solcher Divisoren besitzt, die zugleich Multipla von R sind.

Product $\omega_\iota \omega_{\iota'}$ wieder in der Form (1) enthalten ist; diese Bedingungen, deren Anzahl $= \frac{1}{2}n(n+1)$ ist, lassen sich am einfachsten zusammenfassen, indem man die Coordinaten h_ι als *veränderlich* ansieht und

$$\omega^2 = 2 \sum H_\iota \omega_\iota \tag{2}$$

setzt, wo nun $H_1, H_2 \ldots H_n$ bestimmte, *mit rationalen Coefficienten* behaftete, ganze homogene quadratische Functionen der Coordinaten bedeuten. Durch diese n Functionen H_ι, auf deren analytische Eigenschaften wir unten zurückkommen werden, ist die Constitution des Körpers Ω vollständig bestimmt, und es lässt sich zunächst zeigen, dass die Zahlen von der Form (1) auch durch Division sich wieder erzeugen. Durch totale Differentiation von (2) erhält man

$$\omega\, d\omega = \sum dH_\iota \omega_\iota; \tag{3}$$

legt man den Coordinaten h_ι und ihren Differentialen dh_ι beliebige rationale Werthe bei, so ist durch die vorstehende Gleichung das Product aus zwei beliebigen Zahlen ω und $d\omega$ des Körpers Ω auf die Form (1) zurückgeführt. Speciell ergiebt sich aus (3)

$$\omega \omega_r = \sum \frac{\partial H_\iota}{\partial h_r} \omega_\iota; \tag{4}$$

legt man nun den Coordinaten h_ι beliebige rationale Werthe bei, welche aber nicht sämmtlich verschwinden, so kann auch der entsprechende Werth der Functional-Determinante

$$H = \sum \pm \frac{\partial H_1}{\partial h_1} \frac{\partial H_2}{\partial h_2} \cdots \frac{\partial H_n}{\partial h_n} \tag{5}$$

nicht verschwinden; denn sonst liessen sich bekanntlich n rationale Zahlen dh_ι, die nicht sämmtlich verschwinden, so bestimmen, dass für jeden Index r

$$dH_r = \sum \frac{\partial H_r}{\partial h_\iota} dh_\iota = 0,$$

und folglich auch $\omega\, d\omega = 0$ würde, während doch keine der beiden Zahlen ω und $d\omega$ verschwindet. Hieraus folgt weiter durch Umkehrung der n Gleichungen (4), dass die n Quotienten $\omega_\iota : \omega$ wieder Zahlen von der Form (1) sind; dasselbe gilt daher auch von jedem Quotienten $\alpha : \omega$, wo α irgend eine Zahl von der Form (1) bedeutet. Mithin bilden alle Zahlen von der Form (1) wirklich einen Körper.

Durch Elimination der n Zahlen ω_ι aus den n Gleichungen (4) ergiebt sich die Gleichung

$$\begin{vmatrix} \frac{\partial H_1}{\partial h_1} - \omega, & \frac{\partial H_2}{\partial h_1} & \cdots & \frac{\partial H_n}{\partial h_1} \\ \frac{\partial H_1}{\partial h_2}, & \frac{\partial H_2}{\partial h_2} - \omega & \cdots & \frac{\partial H_n}{\partial h_2} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial H_1}{\partial h_n}, & \frac{\partial H_2}{\partial h_n} & \cdots & \frac{\partial H_n}{\partial h_n} - \omega \end{vmatrix} = 0 \qquad (6)$$

mithin ist jede Zahl ω des Körpers Ω die Wurzel einer (von der Wahl der Basis unabhängigen) Gleichung $n$ten Grades mit rationalen Coefficienten, also eine *algebraische Zahl*, und es lässt sich leicht zeigen, dass in dem Körper Ω auch Zahlen existiren, welche keiner Gleichung mit rationalen Coefficienten von niedrigerem als dem $n$ten Grade genügen, für welche also die vorstehende Gleichung *irreductibel* ist*). Bedeutet θ eine solche Zahl, so bilden

---

*) Der Beweis dieser Behauptung kann z. B. auf das folgende Lemma gestützt werden:

Genügt eine homogene lineare Function $\omega = \Sigma h_\iota \omega_\iota$ der n Variabeln h_ι einer Identität von der Form

$$A\omega^m + A_1 \omega^{m-1} + \cdots + A_m = 0, \qquad (1)$$

wo $A, A_1 \ldots A_m$ ganze Functionen der Variabeln h_ι mit *rationalen* Coefficienten bedeuten, die nicht sämmtlich identisch verschwinden, und ist der Grad m *kleiner* als die Anzahl n der Variabeln, so sind die n Grössen ω_ι von einander *abhängig*.

Durch totale Differentiation der Identität (1) ergiebt sich zunächst

$$M d\omega + \omega^m dA + \omega^{m-1} dA_1 + \cdots + dA_m = 0, \qquad (2)$$

wo zur Abkürzung

$$M = mA\omega^{m-1} + (m-1)A_1 \omega^{m-2} + \cdots + A_{m-1}$$

gesetzt ist. Man kann nun offenbar annehmen, dass keine solche Identität (1) von noch niedrigerm Grade als m existirt, dass also das Product AM nicht identisch verschwindet; nun lege man, was stets möglich ist, den Variabeln h_ι solche rationale Werthe bei, für welche AM einen von Null verschiedenen Werth erhält; hierauf kann man, weil $m < n$ ist, den n Differentialen dh_ι solche rationale Werthe beilegen, welche den m homogenen linearen Gleichungen

$$A\,dA_1 = A_1 dA,\ A\,dA_2 = A_2 dA \ldots A\,dA_m = A_m dA$$

genügen und nicht sämmtlich verschwinden; multiplicirt man nun (1) mit dA, (2) mit A, und subtrahirt, so folgt $AMd\omega = 0$, also auch $d\omega = \Sigma dh_\iota \omega_\iota = 0$, was zu beweisen war.

Hieraus folgt zunächst, dass, wenn die Grössen ω_ι und ω wieder ihre alte Bedeutung erhalten, die aus den Coordinaten der n Grössen $1, \omega, \omega^2 \ldots \omega^{n-1}$ gebildete Determinante D, welche eine homogene Function der

offenbar die Potenzen $1, \theta, \theta^2 \ldots \theta^{n-1}$ ebenfalls eine Basis des Körpers Ω, und Ω ist das System aller Zahlen, welche sich durch beliebige Wiederholung der vier arithmetischen Grundoperationen aus θ ableiten lassen. Substituirt man nun für θ der Reihe nach alle Wurzeln derselben irreductibelen Gleichung, so entstehen ebensoviele entsprechende Körper welche offenbar mit Ω und folglich auch mit einander conjugirt sind, und es liesse sich leicht zeigen, dass ausser diesen Körpern kein anderer mit Ω conjugirt ist. Dabei bemerken wir aber, um Missverständnissen vorzubeugen, dass diese n Körper, was ihren gesammten Zahleninhalt anbetrifft, sehr wohl theilweise oder auch sämmtlich identisch sein können, obgleich sie durch n *verschiedene* Substitutionen aus einem von ihnen hervorgehen *).

Da nun vermöge des Begriffes conjugirter Körper die Gleichungen (4) gültig bleiben, wenn die Zahlen des Körpers Ω durch die entsprechenden Zahlen eines conjugirten Körpers ersetzt werden, so folgt leicht, dass die sämmtlichen Wurzeln der Gleichung (6) die mit ω conjugirten Zahlen sind. Bezeichnet man daher mit $N(\omega)$ die sogenannte *Norm* der Zahl ω, d. h. das Product aus allen n conjugirten Wurzeln, die auch gruppenweise einander gleich sein können, so ist zufolge (6)

$$N(\omega) = H, \tag{7}$$

d. h. die homogene Function H ist das Product aus n conjugirten Factoren ersten Grades mit algebraischen Coefficienten. Aus dieser

---

Variabeln h_i vom Grade $\frac{1}{2}n(n-1)$ ist, nicht identisch verschwinden kann, weil sonst ω einer Identität von der obigen Form (1) und von niedrigerem Grade als n genügte, und folglich die Grössen ω_i von einander abhängig wären. Giebt man nun den Coordinaten h_i solche rationale Werthe, für welche D einen von Null verschiedenen Werth erhält, so folgt unmittelbar, dass die entsprechende Zahl ω des Körpers Ω die Wurzel einer irreductibeln Gleichung $n$ten Grades ist.

Jeder Lösung der Gleichung $D = 0$ in rationalen Zahlen h_i entspricht eine Zahl ω, welche einem Divisor des Körpers Ω von niedrigerem als dem $n$ten Grade angehört; der Grad eines solchen Divisors ist immer ein Divisor von n.

*) Durch die weitere Verfolgung dieses Gegenstandes gelangt man unmittelbar zu den von *Galois* in die Algebra eingeführten Principien (*Sur les conditions de résolubilité des équations par radicaux*; Journ. de Math. p. p. Liouville. T. XI. 1846); hierbei ist es zweckmässig, zunächst die einfachen Reciprocitätsgesetze aufzusuchen, welche zwischen irgend zwei solchen Körpern wie Ω, ihrem grössten gemeinschaftlichen Divisor und ihrem kleinsten gemeinschaftlichen Multiplum herrschen.

Definition geht unmittelbar der Satz hervor: *die Norm eines Productes ist immer gleich dem Product aus den Normen der Factoren.* Setzt man ferner

$$N(\omega) = \omega\,\omega', \tag{8}$$

so ist ω', weil $N(\omega)$ als rationale Zahl in Ω enthalten ist, ebenfalls eine Zahl des Körpers Ω, was auch aus (6) hervorgeht, und zwar ist

$$N(\omega') = N(\omega)^{n-1}; \tag{9}$$

nennen wir ω' die *zu ω adjungirte Zahl**), so ist die zu ω' adjungirte Zahl $= \omega\,N(\omega)^{n-2}$.

Sind $\alpha_1, \alpha_2 \ldots \alpha_n$ beliebige Zahlen des Körpers Ω, nnd bedeuten $\beta_\iota, \gamma_\iota \ldots \lambda_\iota$ die übrigen $(n-1)$ mit α_ι conjugirten Zahlen, so setzen wir zur Abkürzung

$$(\Sigma \pm \alpha_1\,\beta_2 \ldots \lambda_n)^2 = \Delta(\alpha_1, \alpha_2 \ldots \alpha_n) \tag{10}$$

und nennen dieses Determinantenquadrat die *Discriminante* der n Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$; sie ist eine symmetrische Function der n mit θ conjugirten Zahlen und folglich eine *rationale* Zahl, und zwar ist

$$\Delta(\alpha_1, \alpha_2 \ldots \alpha_n) = m^2\,\Delta(\omega_1, \omega_2 \ldots \omega_n), \tag{11}$$

wo m die aus den Coordinaten der Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ gebildete Determinante bedeutet; da die Discriminante $\Delta(1, \theta, \theta^2 \ldots \theta^{n-1})$ bekanntlich das Product aller Differenzen zwischen den mit θ conjugirten Zahlen nnd folglich von Null verschieden ist (weil eine irreductibele Gleichnng nur ungleiche Wurzeln haben kann), so ist $\Delta(\alpha_1 \ldots \alpha_n)$ stets und nur dann $= 0$, wenn die Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ von einander abhängig sind. Endlich ist allgemein

$$\Delta(\omega\alpha_1, \omega\alpha_2 \ldots \omega\alpha_n) = N(\omega)^2\,\Delta(\alpha_1, \alpha_2 \ldots \alpha_n). \tag{12}$$

II. Im Vorhergehenden sind die Begriffe und Sätze entwickelt, deren wir in der Folge bedürfen; zur Erläuterung mögen aber hier noch die wichtigsten und nächstliegenden Resultate aus dem grossen Reichthume analytischer Entwicklungen mitgetheilt werden, welche sich an die Betrachtung der Functionen H_ι anknüpfen. Zwischen diesen n Functionen bestehen fundamentale Relationen, welche man erhält, wenn man das Product aus *drei* beliebigen Zahlen des Körpers Ω auf alle möglichen Arten bildet (vergl. §§. 1, 2). Bedeutet d' wieder eine beliebige Variation, so ist zufolge (4)

---

*) Dieser Ausdruck wird hier in ganz anderer Bedeutung gebraucht, wie von *Galois*.

$$d'\omega\,\omega_r = \Sigma\, d'\left(\frac{\partial H_\iota}{\partial h_r}\right)\omega_\iota;$$

multiplicirt man nun (3) mit $d'\omega$, und ersetzt die Producte $d'\omega\,\omega_\iota$ der vorstehenden Gleichung gemäss durch Summen, so folgt

$$\omega\, d\omega\, d'\omega = \Sigma\, dH_\iota d'\left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right)\omega_{\iota'};$$

da die linke Seite symmetrisch in Bezug auf d und d' ist, und da die n Zahlen $\omega_{\iota'}$ unabhängig sind, so ergiebt sich, dass die Functionen H_ι den n Differentialgleichungen

$$\Sigma\, dH_\iota d'\left(\frac{\partial H_r}{\partial h_\iota}\right) = \Sigma\, d'H_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right) \tag{13}$$

genügen, wo r irgend einen der Indices $1, 2 \ldots n$ bedeutet. Um die Bedeutung dieser Relationen mehr hervortreten zu lassen, wollen wir sie den folgenden Entwicklungen zu Grunde legen, ohne den Zusammenhang der Functionen H_ι mit dem Körper Ω zu benutzen.

Zunächst wollen wir zeigen, dass die Functionaldeterminante H, welche zufolge ihrer Definition (5) eine ganze homogene Function $n$ten Grades mit rationalen Coefficienten ist, sich durch Multiplication reproducirt; gehen die Formen K und L dadurch aus H hervor, dass die Coordinaten h_ι resp. durch dh_ι und durch dH_ι ersetzt werden, so ist

$$L = HK; \tag{14}$$

denn wenn man die Coordinaten h_ι durch dh_ι ersetzt, so geht jede homogene lineare Function

$$\frac{\partial H_r}{\partial H_s} \quad \text{in} \quad d\left(\frac{\partial H_r}{\partial h_s}\right),$$

und folglich H in

$$K = \Sigma \pm d\left(\frac{\partial H_1}{\partial h_1}\right) d\left(\frac{\partial H_2}{\partial h_2}\right) \cdots d\left(\frac{\partial H_n}{\partial h_n}\right)$$

über; werden aber die Coordinaten h_ι durch die bilinearen Functionen dH_ι ersetzt, so geht zufolge (13)

$$\frac{\partial H_r}{\partial h_s} \quad \text{in} \quad \Sigma\, \frac{\partial}{\partial h_s}\left(\frac{\partial H_r}{\partial h_\iota}\right) dH_\iota = \Sigma\, \frac{\partial H_\iota}{\partial h_s}\, d\left(\frac{\partial H_r}{\partial h_\iota}\right),$$

und folglich H in $L = HK$ über, was zu beweisen war. Dies ist der schon oben angeführte Satz über die Norm eines Productes.

Bedeutet φ eine willkürliche Function der Coordinaten h_ι, und definirt man die Variation δ dadurch, dass

$$\delta\varphi = \Sigma \frac{\partial\varphi}{\partial H_\iota} h_\iota, \quad \text{also} \quad \delta H_\iota = h_\iota \tag{15}$$

wird, so ergiebt sich aus (13), wenn man d' durch δ ersetzt,

$$\Sigma\, dH_\iota \delta\left(\frac{\partial H_r}{\partial h_\iota}\right) = \Sigma\, h_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right) = dH_r,$$

weil H_r eine homogene Function zweiten Grades ist, mithin

$$\delta\left(\frac{\partial H_r}{\partial h_s}\right) = 1 \quad \text{oder} \quad = 0 \tag{16}$$

je nachdem r und s gleich oder ungleich sind; hieraus folgt, dass die n Variationen δh_ι *constante, rationale Zahlen* sind. Wird ferner die Variation δ' durch

$$\delta'\varphi = H\, \Sigma \frac{\partial\varphi}{\partial H_\iota} \delta h_\iota, \quad \text{also} \quad \delta' H_\iota = H\delta h_\iota \tag{17}$$

definirt, so ergiebt sich, wenn man in (13) d' durch δ' ersetzt,

$$\Sigma\, dH_\iota \delta'\left(\frac{\partial H_r}{\partial h_\iota}\right) = H\, \Sigma\, \delta h_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right) = Hd\, \Sigma \frac{\partial H_r}{\partial h_\iota} \delta h_\iota$$
$$= Hd\delta H_r = Hdh_r,$$

folglich

$$\delta'\left(\frac{\partial H_r}{\partial h_s}\right) = H \frac{\partial h_r}{\partial H_s}; \tag{18}$$

da nun der Ausdruck rechter Hand der Coefficient des Elementes

$$\frac{\partial H_s}{\partial h_r}$$

in der Determinante H, also eine *ganze homogene Function* $(n-1)$*ten Grades* der Coordinaten h_ι mit rationalen Coefficienten ist, so gilt dasselbe von den Grössen

$$h'_r = \delta' h_r = H\, \Sigma \frac{\partial h_r}{\partial H_\iota} \delta h_\iota, \tag{19}$$

und umgekehrt geht aus (18) hervor, dass die Coefficienten der einzelnen n^2 Elemente in der Determinante H sich als homogene lineare Functionen der soeben definirten n Grössen h'_ι darstellen lassen. Wir wollen, wenn φ eine beliebige Function der Coordinaten h_ι bedeutet, mit φ' dieselbe Function der Grössen h'_ι bezeichnen; dann lautet die Gleichung (18)

$$\frac{\partial H'_r}{\partial h'_\iota} = H \frac{\partial h_r}{\partial H_\iota}, \tag{20}$$

und hieraus folgt zugleich

$$H' = H^{n-1}; \quad H \frac{\partial h'_\iota}{\partial H'_r} = \frac{\partial H_\iota}{\partial h_r}. \tag{21}$$

Da H eine Functionaldeterminante ist, so ist bekanntlich*)

$$d \log H = \Sigma \frac{\partial d H_\iota}{\partial H_\iota} - \Sigma \frac{\partial d h_\iota}{\partial h_\iota},$$

und folglich ergiebt sich unter Berücksichtigung von (13)

$$\Sigma \frac{\partial \log H}{\partial h_\iota} d H_\iota = \Sigma \frac{\partial}{\partial H_{\iota'}} \left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right) d H_\iota$$

$$= \Sigma\, d\left(\frac{\partial H_{\iota'}}{\partial h_\iota}\right) \frac{\partial H_\iota}{\partial H_{\iota'}} = d\, \Sigma \frac{\partial H_\iota}{\partial h_\iota};$$

führt man daher die *homogene lineare Function*

$$S = \Sigma \frac{\partial H_\iota}{\partial h_\iota} \tag{22}$$

ein, so ist

$$\Sigma \frac{\partial \log H}{\partial h_\iota} d H_\iota = d S; \quad \frac{\partial \log H}{\partial h_r} = \frac{\partial S}{\partial H_r}, \tag{23}$$

also mit Rücksicht auf (20)

$$\frac{\partial H}{\partial h_r} = H\, \Sigma \frac{\partial S}{\partial h_\iota} \frac{\partial h_\iota}{\partial H_r} = \Sigma \frac{\partial S}{\partial h_\iota} \frac{\partial H'_\iota}{\partial h'_r};$$

man führe daher die *ganze homogene Function zweiten Grades*

$$T = \Sigma \frac{\partial S}{\partial h_\iota} H_\iota \tag{24}$$

ein, so wird

$$\frac{\partial H}{\partial h_r} = \frac{\partial T'}{\partial h'_r}; \quad d H = \Sigma \frac{\partial T'}{\partial h'_\iota} d h_\iota, \tag{25}$$

mithin sind auch die Derivirten der Form H darstellbar als homogene lineare Functionen der in (19) definirten Grössen h'_ι, und rückwärts diese durch jene. Da ferner zufolge (20)

---

*) *Jacobi: De determinantibus functionalibus* §. 9 (Crelle's Journal XXII); in der obigen Form ist auch der Fall berücksichtigt, dass die Differentiale $d h_\iota$ Functionen von den Veränderlichen h_ι sind. Ersetzt man d durch δ', so folgt aus (17) und (19) unmittelbar

$$\Sigma \frac{\partial h'_\iota}{\partial h_\iota} = 0.$$

$$\Sigma \frac{\partial H'_\iota}{\partial h'_s} \frac{\partial H_r}{\partial h_\iota} = H \text{ oder } = 0$$

ist, je nachdem r und s gleich oder ungleich sind, so folgt durch Multiplication mit h'_s oder dh'_s und Summation in Bezug auf s

$$2 \Sigma H'_\iota \frac{\partial H_r}{\partial h_\iota} = Hh'_r; \quad \Sigma dH'_\iota \frac{\partial H_r}{\partial h_\iota} = Hdh'_r$$

und hieraus durch Differentiation

$$h'_r dH - Hdh'_r = 2 \Sigma H'_\iota d\left(\frac{\partial H_r}{\partial h_\iota}\right). \tag{26}$$

Mit Hülfe von (25) und (26) ist man im Stande, auch die Differentiale höherer Ordnung von H zu bilden; auf diese Weise findet man

$$Hdd'H - dHd'H = 2H \Sigma \frac{\partial H}{\partial h_\iota} dd'h_\iota - 2 \Sigma \frac{\partial^2 T}{\partial h_\iota \partial h_{\iota'}} H'_\iota dd'H_{\iota'}; \tag{27}$$

ausserdem ergiebt sich aus Gleichung (26), welcher man mit Hülfe von (13) auch die Form

$$h'_r dH - Hdh'_r = \Sigma \frac{\partial H'_\iota}{\partial h'_{\iota'}} \frac{\partial H'_r}{\partial h'_\iota} dh_{\iota'}$$

geben kann, die Functionaldeterminante

$$\Sigma \pm \frac{\partial h'_1}{\partial h_1} \frac{\partial h'_2}{\partial h_2} \cdots \frac{\partial h'_n}{\partial h_n} = (-1)^{n-1}(n-1) H^{n-2} \tag{28}$$

und folglich aus (25) die Hesse'sche Determinante der Form H, nämlich

$$\Sigma \pm \frac{\partial^2 H}{\partial h_1^2} \cdots \frac{\partial^2 H}{\partial h_n^2} = (-1)^{n-1}(n-1) H^{n-2} \Sigma \pm \frac{\partial^2 T}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2}. \tag{29}$$

Aus den Gleichungen (16), (22), (24), (25), (26), (27) ergeben sich unmittelbar folgende auf die Variation δ bezüglichen Resultate:

$$\begin{gathered} \delta S = n; \quad \delta T = S; \quad h'_r \delta H - H \delta h'_r = 2 H'_r; \\ \delta H = S'; \quad \delta' H = \delta H^2 - H \delta^2 H = 2 T'. \end{gathered} \tag{30}$$

III. Alle diese Sätze sind abgeleitet aus der Voraussetzung, dass das System der n ganzen homogenen Functionen H_ι vom zweiten Grade den Bedingungen (13) genügt, und dass ihre Functionaldeterminante H nicht identisch verschwindet; fügt man noch die Voraussetzung hinzu, dass die Coefficienten dieser Functionen

rationale Zahlen sind, und dass die Form H *irreductibel*, d. h. nicht zerlegbar ist in Factoren niedrigeren Grades, deren Coefficienten ebenfalls rationale Zahlen sind, so lässt sich umgekehrt beweisen, dass zu diesem Functionensystem ein algebraischer Zahlkörper Ω von der oben betrachteten Art gehört. Der Kürze halber führen wir eine Charakteristik ε ein, welche folgenden Sinn hat: ist φ irgend eine Function der Coordinaten h_ι, und ersetzt man die letzteren durch $h_\iota - \omega\,\delta h_\iota$, wo ω vorläufig eine *willkürliche* Function bedeutet, so geht φ in eine neue Function über, welche mit $\varepsilon(\varphi)$ bezeichnet werden soll. Aus dieser Definition folgt sofort

$$d\,\varepsilon(\varphi) = \varepsilon(d\varphi) - \varepsilon(\delta\varphi)\,d\omega; \tag{31}$$

unter der Voraussetzung, dass die Differentiale dh_ι *constant* sind. Hierauf definire man die Function ω als Wurzel der Gleichung $n$ten Grades

$$\varepsilon(H) = 0, \tag{32}$$

welche zufolge (16) vollständig mit der Gleichung (6) übereinstimmt, so lässt sich beweisen, dass ω eine *ganze* (homogene) Function ersten Grades, d. h. dass $dd'\omega = 0$ ist, wenn die Differentiale dh_ι, $d'h_\iota$ als constant vorausgesetzt werden. In der That ergiebt sich durch successive Differentiation der Identität (32) nach der in (31) ausgesprochenen Regel

$$\varepsilon(\delta H)\,d\omega = \varepsilon(dH) \tag{33}$$

und

$$\varepsilon(\delta H)^3\,dd'\omega = \varepsilon(R), \tag{34}$$

wo zur Abkürzung die homogene Function $(3n-4)$ten Grades

$$\left\{\begin{array}{l} \delta H^2\,dd'H + \delta^2 H\,dH\,d'H \\ -\,\delta H\,dH\,d'\delta H - \delta H\,d'H\,d\delta H \end{array}\right\} = R$$

gesetzt ist. Dass diese Function R durch H theilbar, in Zeichen, dass $R \equiv 0$ ist*), ergiebt sich auf folgende Weise.

Aus (30) folgt

$$h'_r\,\delta H = 2\,H'_r + H\delta h'_r \equiv 2\,H'_r$$

ferner

$$h'_r\,\delta^2 H = 2\,\delta H'_r + H\delta^2 h'_r \equiv 2\,\delta H'_r$$

und hieraus durch Elimination von h'_r

$$\delta^2 H\,H'_r - \delta H\,\delta H'_r \equiv 0;$$

*) Dies gilt allgemein von dem Ausdrucke
$d'H\,d'''H\,dd''H + dH\,d''H\,d'd'''H - d'''H\,dH\,d'd''H - d'H\,d''H\,dd'''H.$

da nun zufolge (27) $dHd'H - Hdd'H$ eine homogene lineare Function der n Grössen H'_ι ist, so folgt auch, dass

$$\delta^2 H(dHd'H - Hdd'H) - \delta H\delta(dHd'H - Hdd'H) \equiv 0$$

ist; die linke Seite unterscheidet sich aber von R nur um Bestandtheile, welche durch H theilbar sind. Mithin ist $R = PH$, wo P eine ganze Function bedeutet, und folglich $\varepsilon(R) = \varepsilon(P)\,\varepsilon(H) = 0$. Da sich nun aus den Voraussetzungen über H beweisen lässt, dass $\varepsilon(\delta H)$ nicht identisch verschwindet, so folgt aus (34) $dd'\omega = 0$, d. h. die Wurzel ω der Gleichung (32) ist eine ganze Function ersten Grades; dass sie zugleich homogen ist, versteht sich von selbst, weil $H, \delta H \ldots \delta^{n-1} H$ und folglich auch ω gleichzeitig mit den Coordinaten h_ι verschwinden. Setzt man nun

$$\frac{\partial \omega}{\partial h_\iota} = \omega_\iota, \quad \omega = \Sigma\, h_\iota \omega_\iota, \tag{1}$$

so ergiebt sich aus (33), dass

$$\Sigma\, \delta h_\iota \omega_\iota = \delta\omega = 1 \tag{35}$$

und

$$\varepsilon\left(\frac{\partial H}{\partial h_\iota}\right) = \varepsilon(\delta H)\,\omega_\iota \tag{36}$$

ist. Da ferner zufolge (23)

$$\Sigma \frac{\partial H}{\partial h_\iota}\, dH_\iota = H dS \equiv 0$$

und

$$\varepsilon(dH_\iota) = dH_\iota - \omega\, d\delta H_\iota = dH_\iota - \omega\, dh_\iota$$

ist, so folgt

$$0 = \varepsilon(H) dS = \Sigma\, \varepsilon\left(\frac{\partial H}{\partial h_\iota}\right) \varepsilon(dH_\iota)$$
$$= \varepsilon(\delta H)\ \Sigma\, \omega_\iota (dH_\iota - \omega\, dh_\iota),$$

mithin

$$\omega\, d\omega = \Sigma\, dH_\iota \omega_\iota, \tag{3}$$

also auch

$$\omega^2 = 2\, \Sigma\, H_\iota \omega_\iota, \tag{2}$$

wodurch wir rückwärts zu unseren ursprünglichen Annahmen zurückgekehrt sind; und man kann auch beweisen — worauf wir hier nicht eingehen wollen — dass aus den Voraussetzungen über H die *Unabhängigkeit* der n Zahlen ω_ι folgt.

Wir fügen diesen Entwicklungen endlich noch folgende leicht zu beweisende Bemerkungen hinzu. Die ausgeführte Form der Gleichung (32) oder (6) ist folgende

$$0 = H - \delta H \frac{\omega}{1} + \delta^2 H \frac{\omega^2}{1.2} - \delta^3 H \frac{\omega^3}{1.2.3} + \cdots; \qquad (37)$$

es ist ferner

$$H = \prod \omega = N(\omega), \qquad (7)$$

wo das Productzeichen Π sich auf alle n Wurzeln ω bezieht; ebenso findet man (wenn man in (3) d durch δ' ersetzt)

$$H = \omega\omega', \qquad (8)$$

wo

$$\omega' = \delta'\omega = \sum h_i'\omega_i \qquad (38)$$

zu ω adjungirt ist, und

$$S = \Sigma\,\omega, \quad 2\,T = \Sigma\,\omega^2, \qquad (39)$$

wo die Summenzeichen sich ebenfalls auf alle n Wurzeln beziehen. Die quadratische Form T ist charakteristisch für die Anzahl der reellen Wurzeln; bildet man ferner die Hesse'sche Determinante des Productes $H = \Pi\,\omega$, so ergiebt sich durch Vergleichung mit (29) die Discriminante

$$\varDelta(\omega_1, \omega_2 \ldots \omega_n) = \Sigma \pm \frac{\partial^2 T}{\partial h_1^2} \cdots \frac{\partial^2 T}{\partial h_n^2}, \qquad (40)$$

was auch umittelbar aus (39) folgt.

§. 160.

Der Inbegriff *aller* algebraischen Zahlen bildet offenbar ebenfalls einen Körper*). Wir wollen nun, indem wir unserem eigent-

*) Dass es ausser den algebraischen noch andere, sogenannte *transcendente* Zahlen giebt, ist meines Wissens zuerst von *Liouville* bewiesen (*Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques;* Journ. de Math. T. XVI. 1851). Man vermuthet, dass die Ludolph'sche Zahl π eine solche transcendente Zahl ist; allein selbst die als specieller Fall hierin enthaltene Behauptung, dass die Quadratur des Zirkels unmöglich sei, ist bis auf den heutigen Tag noch nicht erwiesen. (Vergl. *Euler: De relatione inter ternas pluresve quantitates instituenda.* §. 10. Opusc. anal. T. II. 1785.)

lichen Gegenstande näher treten, eine Zahl α eine *ganze algebraische Zahl* nennen, wenn sie die Wurzel einer Gleichung ist, deren Coefficienten rationale ganze Zahlen sind, wobei wir ein- für allemal bemerken, dass wir unter den *Coefficienten* einer Function $m$ten Grades

$$F(x) = cx^m + c_1 x^{m-1} + c_2 x^{m-2} + \cdots + c_m$$

oder der Gleichung $F(x) = 0$ stets die m Quotienten

$$-\frac{c_1}{c}, \quad +\frac{c_2}{c} \cdots (-1)^m \frac{c_m}{c}$$

verstehen. Aus dieser Erklärung folgt zunächst, dass eine rationale Zahl stets und nur dann eine ganze algebraische Zahl ist, wenn sie eine ganze Zahl im gewöhnlichen Sinne des Wortes ist (vergl. §. 5, 4.); diese Zahlen wollen wir von jetzt ab *rationale ganze Zahlen*, alle algebraischen ganzen Zahlen aber kurz *ganze Zahlen* nennen. Dieses vorausgeschickt, schreiten wir zum Beweise der folgenden Fundamentalsätze.

1. *Die Summe, die Differenz und das Product zweier ganzen Zahlen α, β sind wieder ganze Zahlen.*

Sind a, b resp. die Grade der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$, deren Coefficienten rationale ganze Zahlen sind, und bezeichnet man mit $\omega_1, \omega_2 \ldots \omega_n$ die sämmtlichen ab Producte von der Form $\alpha^{a'}\beta^{b'}$, wo a' irgend eine der Zahlen $0, 1, 2 \ldots (a-1)$, und b' irgend eine der Zahlen $0, 1, 2 \ldots (b-1)$ bedeutet, so wird, wenn $\omega = \alpha + \beta$, oder $= \alpha - \beta$, oder $= \alpha\beta$ ist, jedes der n Producte $\omega\omega_1, \omega\omega_2 \ldots \omega\omega_n$ mit Zuziehung der Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0$ auf die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ gebracht werden können, wo $r_1, r_2 \ldots r_n$ rationale ganze Zahlen sind. Eliminirt man die n Grössen $\omega_1, \omega_2 \ldots \omega_n$ aus diesen n Gleichungen, so ergiebt sich für ω eine Gleichung vom $n$ten Grade (wie (6) in §. 159), deren Coefficienten rationale ganze Zahlen sind, was zu beweisen war (vergl. §. 139).

2. Die ganze Zahl α heisst *theilbar* durch die ganze Zahl β, oder ein *Multiplum* von β, wenn der Quotient $\alpha : \beta$ ebenfalls eine ganze Zahl ist; umgekehrt heisst β ein *Divisor* oder *Theiler* von α (vergl. §. 3). Ebenso setzen wir $\alpha \equiv \beta \pmod{\gamma}$, wenn $\alpha - \beta$ durch γ theilbar ist, und nennen α, β *congruent nach dem Modul* γ (vergl. §. 17). Man erkennt sofort (zufolge 1.), dass die Sätze des §. 3 und auch die des §. 17 (mit *vorläufiger* Ausnahme von 6. und 8.; vergl. §. 164, 3.) ihre Gültigkeit behalten.

3. *Jede Wurzel ω einer Gleichung, deren Coefficienten ganze Zahlen sind, ist ebenfalls eine ganze Zahl.*

Ist ω die Wurzel einer Gleichung $m$ten Grades $F(\omega) = 0$, deren Coefficienten $\alpha, \beta \ldots$ ganze Zahlen sind, sind ferner $a, b \ldots$ resp. die Grade der mit rationalen ganzen Coefficienten behafteten Gleichungen $\varphi(\alpha) = 0$, $\psi(\beta) = 0 \ldots$, so führe man die sämmtlichen $m a b \ldots$ Producte $\omega_1, \omega_2 \ldots \omega_n$ von der Form $\omega^{m'} \alpha^{a'} \beta^{b'} \ldots$ ein, wo die ganzen rationalen Exponenten den Bedingungen $0 \leqq m' < m$, $0 \leqq a' < a$, $0 \leqq b' < b \ldots$ genügen; dann lässt sich vermöge der Gleichungen $F(\omega) = 0$, $\varphi(\alpha) = 0$, $\psi(\beta) = 0 \ldots$ jedes der n Producte $\omega\omega_1$, $\omega\omega_2 \ldots \omega\omega_n$ wieder in die Form $r_1\omega_1 + r_2\omega_2 + \cdots + r_n\omega_n$ bringen, wo $r_1, r_2 \ldots r_n$ rationale ganze Zahlen bedeuten, und hieraus folgt unmittelbar die Richtigkeit des Satzes.

Ist daher z. B. α eine ganze Zahl, und r eine beliebige (ganze oder gebrochene) *positive* rationale Zahl, so ist auch α^r eine ganze Zahl (vergl. §. 5, 4.).

4. Bekanntlich lassen sich die Begriffe der Theilbarkeit und des Vielfachen von den ganzen rationalen Zahlen unmittelbar auf die ganzen rationalen Functionen übertragen, und es giebt einen Algorithmus zur Auffindung des grössten gemeinschaftlichen Divisors $\varphi(x)$ zweier gegebenen Functionen $F(x)$, $f(x)$, welcher demjenigen der Zahlentheorie (§. 4) vollständig analog ist. Sind die Coefficienten von $F(x)$ und $f(x)$ sämmtlich in einem Körper K enthalten, so werden auch die Coefficienten von $\varphi(x)$ Zahlen des Körpers K sein, weil sie durch Addition, Multiplication, Subtraction und Division aus den Coefficienten von $F(x)$ und $f(x)$ entstehen. Hieraus folgt leicht, dass, wenn α die Wurzel einer solchen Gleichung $F(\alpha) = 0$ ist, deren Coefficienten Zahlen des Körpers K sind, nothwendig auch eine solche Gleichung $\varphi(\alpha) = 0$ von *niedrigstem Grade* existiren muss, welche *irreductibel in K* heissen soll und welche offenbar keine anderen Wurzeln besitzen kann als die Gleichung $F(\alpha) = 0$. Hieraus folgt der Satz:

Ist α eine ganze Zahl, und K ein bestimmter Körper, so sind alle Coefficienten der in K irreductibelen Gleichung $\varphi(\alpha) = 0$ ganze Zahlen.

Denn weil α eine ganze Zahl, also die Wurzel einer Gleichung $F(\alpha) = 0$ ist, deren Coefficienten rationale ganze Zahlen und folg-

lich auch Zahlen des Körpers K sind (§. 159), so kann die in K irreductibele Gleichung $\varphi(\alpha) = 0$, welcher α genügt, nur ganze Zahlen zu Wurzeln haben; da aber die Coefficienten einer Gleichung durch Addition und Multiplication aus ihren Wurzeln entstehen, so sind (zufolge 1.) auch die Coefficienten der Gleichung $\varphi(\alpha) = 0$ ganze Zahlen, was zu beweisen war.

Der einfachste Fall, in welchem K der Körper der rationalen Zahlen ist, findet sich bei *Gauss**).

5. *Ist ϱ irgend eine algebraische Zahl, so giebt es immer unendlich viele (von Null verschiedene) rationale ganze Zahlen h von der Beschaffenheit, dass $h\varrho$ eine ganze Zahl wird, und zwar stimmen diese sämmtlichen Zahlen h mit den sämmtlichen rationalen Vielfachen der kleinsten unter ihnen überein.*

Da ϱ eine algebraische Zahl, also die Wurzel einer Gleichung von der Form

$$c\varrho^m + c_1\varrho^{m-1} + c_2\varrho^{m-2} + \cdots + c_m = 0$$

ist, wo $c, c_1, c_2 \ldots c_m$ rationale ganze Zahlen bedeuten, so ergiebt sich durch Multiplication mit c^{m-1}, dass $c\varrho$ eine ganze Zahl ist. Sind ferner $a\varrho$, $b\varrho$ ganze Zahlen, wo a, b rationale ganze Zahlen bedeuten, deren grösster gemeinschaftlicher Theiler $= h$ ist, so folgt leicht (aus 1. und §. 4), dass auch $h\varrho$ eine ganze Zahl ist. Hieraus ergiebt sich unmittelbar der zu beweisende Satz.

6. Versteht man unter einer *Einheit* eine ganze Zahl ε, welche in *allen* ganzen Zahlen aufgeht, so ist zunächst erforderlich, dass sie auch in 1 aufgeht, dass also $1 = \varepsilon\varepsilon'$, und ε' eine ganze Zahl ist; wenn nun

$$\varepsilon^m + c_1\varepsilon^{m-1} + \cdots + c_m = 0$$

die im Körper der rationalen Zahlen irreductibele Gleichung ist, welcher ε genügt, so muss (zufolge 4.) $c_m = \pm 1$ sein, weil ε' der ebenfalls irreductibelen Gleichung

$$c_m\varepsilon'^m + c_{m-1}\varepsilon'^{m-1} + \cdots + c_1\varepsilon' + 1 = 0$$

genügt; umgekehrt, ist dies der Fall, so geht ε in 1 und folglich in allen ganzen Zahlen auf, ist also eine Einheit. Die Anzahl der Einheiten ist offenbar unbegrenzt.

Ist α theilbar durch α', und sind ε, ε' irgend welche Einheiten, so ist offenbar auch $\varepsilon\alpha$ durch $\varepsilon'\alpha'$ theilbar; hinsichtlich der Theilbarkeit verhalten sich daher alle Zahlen $\varepsilon\alpha$, welche den sämmt-

*) *D. A.* art. 42.

lichen Einheiten ε entsprechen, genau wie α. Zwei ganze Zahlen, deren Quotient keine Einheit ist, wollen wir *wesentlich verschieden* nennen.

7. Will man nun den Begriff der *Primzahl* so fassen, dass sie ausser sich selbst und den Einheiten keine wesentlich verschiedene Theiler besitzt und auch selbst keine Einheit ist, so erkennt man sofort, dass gar keine solche Zahl existirt; ist nämlich α eine ganze Zahl, aber keine Einheit, so besitzt sie immer unendlich viele wesentlich verschiedene Divisoren, z. B. die Zahlen $\sqrt{\alpha}$, $\sqrt[3]{\alpha}$, $\sqrt[4]{\alpha}$ u. s. f., welche (zufolge 3.) ganze Zahlen sind.

Dagegen lässt sich der Begriff von *relativen Primzahlen* vollständig definiren, und diese Frage wird uns überhaupt auf den richtigen Weg leiten, welcher bei den ferneren Untersuchungen einzuschlagen ist. Da von einem grössten gemeinschaftlichen Theiler zweier ganzen Zahlen *vorläufig* (vergl. §. 164, 3.) nicht gesprochen werden kann, so ist es auch unmöglich, die Definition von relativen Primzahlen so zu fassen, wie sie in der Theorie der rationalen Zahlen aufgestellt wird (§. 5); aber aus dieser Definition ergaben sich mehrere Sätze, deren jeder umgekehrt das Verhalten zweier relativen Primzahlen vollständig charakterisirt, ohne die Kenntniss ihrer sämmtlichen Divisoren vorauszusetzen. Ein solcher Satz ist z. B. der folgende (§. 7): Sind a, b relative Primzahlen, so ist jede durch a und b theilbare Zahl auch durch ab theilbar. Dieser Satz lässt sich in der That umkehren: Ist jede durch a und b theilbare Zahl auch durch ab theilbar, so sind a, b relative Primzahlen. Hätten nämlich die beiden Zahlen $a = ha'$, $b = hb'$ einen gemeinschaftlichen Theiler $h > 1$, so wäre $ha'b'$ eine durch a und b, aber nicht durch ab theilbare Zahl.

Diese Betrachtung veranlasst uns, folgende für das Gebiet aller ganzen algebraischen Zahlen gültige Erklärung aufzustellen:

Zwei von Null verschiedene ganze Zahlen α, β heissen relative Primzahlen, wenn jede durch α und β theilbare Zahl auch durch $\alpha\beta$ theilbar ist.

Vor Allem bemerken wir, dass zwei relative Primzahlen im alten Sinne des Wortes, d. h. zwei rationale ganze Zahlen a, b, deren grösster gemeinschaftlicher Divisor $= 1$ ist, auch im neuen Sinne relative Primzahlen bleiben; ist nämlich eine ganze algebraische Zahl γ theilbar durch a und b, so ist der Quotient $\varrho = \gamma : ab$ eine algebraische Zahl der Art, dass $a\varrho$ und $b\varrho$ ganze Zahlen sind; mithin muss (zufolge 5.) auch ϱ eine ganze Zahl, also γ theilbar durch

ab sein, was zu beweisen war. Dass ferner umgekehrt zwei relative Primzahlen im neuen Sinne des Wortes, welche zugleich rational sind, auch relative Primzahlen im alten Sinne sind, versteht sich zufolge der der neuen Erklärung vorausgeschickten Erörterung von selbst.

Wir nennen ferner die ganzen Zahlen $\alpha, \beta, \gamma, \delta \ldots$ kurz relative Primzahlen, wenn jede von ihnen relative Primzahl zu jeder der andern ist (vergl. §. 6); ist dann eine ganze Zahl ω durch jede von ihnen theilbar, so ist sie auch durch ihr Product theilbar (vergl. §. 7), weil, wie man leicht findet, auch der folgende Satz (§. 5, 3.) seine Gültigkeit behält: Ist jede der Zahlen $\alpha', \beta', \gamma' \ldots$ relative Primzahl zu jeder der Zahlen $\alpha'', \beta'', \gamma'', \delta'' \ldots$, so sind auch die Producte $\alpha'\beta'\gamma' \ldots$ und $\alpha''\beta''\gamma''\delta'' \ldots$ relative Primzahlen und umgekehrt.

Aber wie soll man definitiv entscheiden, ob zwei gegebene ganze Zahlen α, β relative Primzahlen sind? Man könnte versuchen, folgenden Weg einzuschlagen. Da α^{-1} und β^{-1} algebraische Zahlen sind, so giebt es (zufolge 5.) immer zwei kleinste positive ganze rationale Zahlen a, b von der Art, dass $a\alpha^{-1}$ und $b\beta^{-1}$ ganze Zahlen, d. h. dass a, b resp. durch α, β theilbar werden; zeigt sich nun, dass a, b relative Primzahlen sind, so sind auch α, β gewiss relative Primzahlen. Aber man muss sich hüten zu glauben, dass auch das Umgekehrte Statt findet, dass also die *kleinsten rationalen Multipla* a, b von zwei relativen Primzahlen α, β nothwendig selbst relative Primzahlen sein müssen. So z. B. sind in der That die beiden conjugirten Zahlen $\alpha = 2 + i$ und $\beta = 2 - i$ relative Primzahlen, und doch ist $a = b = 5$. Eine wesentliche Reduction unserer Aufgabe wird aber durch den folgenden Satz bewirkt:

Wenn zwei ganze Zahlen α, β sich in einem Körper K, dem sie selbst angehören, als relative Primzahlen bewähren, d. h. wenn jede durch α und β theilbare Zahl des Körpers K auch durch $\alpha\beta$ theilbar ist; so sind α, β wirklich relative Primzahlen.

Ist nämlich ω irgend eine durch α und durch β theilbare ganze Zahl, und ist

$$\omega^m + \gamma_1 \omega^{m-1} + \gamma_2 \omega^{m-2} + \cdots + \gamma_m = 0$$

die in K irreductibele Gleichung, welcher ω genügt, so sind (zufolge 4.) die Zahlen $\gamma_1, \gamma_2 \ldots \gamma_m$ ganze Zahlen des Körpers K; da ferner

die ganzen Zahlen $\alpha' = \omega : \alpha$ und $\beta' = \omega : \beta$ resp. den in K irreductibelen Gleichungen

$$(\alpha\alpha')^m + \gamma_1(\alpha\alpha')^{m-1} + \cdots + \gamma_m = 0$$

$$(\beta\beta')^m + \gamma_1(\beta\beta')^{m-1} + \cdots + \gamma_m = 0$$

genügen, so sind (zufolge 4.) auch die Quotienten $\gamma_n : \alpha^n$ und $\gamma_n : \beta^n$ ganze Zahlen des Körpers K; da ferner nach Voraussetzung jede durch α und β theilbare Zahl des Körpers K auch durch $\alpha\beta$ theilbar ist, so ergiebt sich leicht, dass auch jede durch α^n und β^n theilbare Zahl γ_n des Körpers K durch $\alpha^n\beta^n$ theilbar, also von der Form $\alpha^n\beta^n\gamma'_n$ ist, wo γ'_n eine ganze Zahl bedeutet; setzt man nun $\omega = \alpha\beta\omega'$, so genügt ω' der Gleichung

$$\omega'^m + \gamma'_1\omega'^{m-1} + \cdots + \gamma'_m = 0,$$

deren Coefficienten ganze Zahlen sind; mithin ist ω' (zufolge 3.) eine ganze Zahl, d. h. ω ist auch theilbar durch $\alpha\beta$, was zu beweisen war.

Hieraus geht hervor, dass man, um das gegenseitige Verhalten zweier ganzen Zahlen α, β zu untersuchen, nur den kleinsten Körper K zu bilden braucht, welchem sie beide angehören; und dieser Körper ist, wie man leicht erkennt, immer von der im vorigen Paragraphen betrachteten Beschaffenheit.

§. 161.

Um den späteren Verlauf der Darstellung nicht zu unterbrechen, schalten wir hier eine sehr allgemeine Betrachtung ein, welche für die nachfolgenden, sowie für viele andere, unserem Gegenstande fremde Untersuchungen von grossem Nutzen ist.

1. Ein System $\mathfrak{a}$ von reellen oder complexen Zahlen α, deren *Summen* und *Differenzen* demselben System $\mathfrak{a}$ angehören, soll ein *Modul* heissen; wenn die Differenz zweier Zahlen ω, ω' in $\mathfrak{a}$ enthalten ist, so wollen wir sie *congruent nach* $\mathfrak{a}$ nennen und dies durch die Congruenz

$$\omega \equiv \omega' \pmod{\mathfrak{a}}$$

andeuten. Solche Congruenzen können addirt, subtrahirt und folglich auch mit beliebigen ganzen rationalen Zahlen multiplicirt werden, wie Gleichungen. Da je zwei einer dritten congruente Zahlen

auch einander congruent sind, so kann man alle existirenden Zahlen in *Classen* (mod. $\mathfrak{a}$) eintheilen, indem man je zwei congruente Zahlen in dieselbe Classe, je zwei incongruente in zwei verschiedene Classen aufnimmt.

2. Wenn alle Zahlen eines Moduls $\mathfrak{a}$ auch Zahlen eines Moduls $\mathfrak{d}$ sind, so heisse $\mathfrak{a}$ ein *Vielfaches* von $\mathfrak{d}$, und $\mathfrak{d}$ ein *Theiler* von $\mathfrak{a}$; oder wir sagen auch, $\mathfrak{d}$ gehe in $\mathfrak{a}$ auf, $\mathfrak{a}$ sei theilbar durch $\mathfrak{d}$. Aus jeder Congruenz $\omega \equiv \omega'$ (mod. $\mathfrak{a}$) folgt auch $\omega \equiv \omega'$ (mod. $\mathfrak{d}$). Offenbar *besteht* $\mathfrak{d}$ aus einer endlichen oder unendlichen Anzahl von Classen (mod. $\mathfrak{a}$).

Sind $\mathfrak{a}$, $\mathfrak{b}$ irgend zwei Moduln, so bilden alle die Zahlen, welche gleichzeitig in $\mathfrak{a}$ und in $\mathfrak{b}$ enthalten sind, das *kleinste* gemeinschaftliche Vielfache $\mathfrak{m}$ von $\mathfrak{a}$ und $\mathfrak{b}$, weil jedes gemeinschaftliche Vielfache von $\mathfrak{a}$ und $\mathfrak{b}$ auch durch den Modul $\mathfrak{m}$ theilbar ist. Durchläuft α alle Zahlen des Moduls $\mathfrak{a}$, β alle Zahlen des Moduls $\mathfrak{b}$, so bilden die Zahlen $\alpha + \beta$ den *grössten* gemeinschaftlichen Theiler von $\mathfrak{a}$ und $\mathfrak{b}$, weil jeder gemeinschaftliche Theiler von $\mathfrak{a}$ und $\mathfrak{b}$ auch in dem Modul $\mathfrak{d}$ aufgeht.

3. Sind $\omega_1, \omega_2 \ldots \omega_n$ gegebene Zahlen, so bilden alle Zahlen von der Form

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n, \tag{1}$$

wo $h_1, h_2 \ldots h_n$ alle ganzen rationalen Zahlen durchlaufen, einen *endlichen* Modul $\mathfrak{o}$, und wir wollen den Complex der n Zahlen $\omega_1, \omega_2 \ldots \omega_n$, mögen sie abhängig oder unabhängig von einander sein, eine *Basis* des Moduls $\mathfrak{o}$ nennen. Dann besteht folgender Satz:

Wenn alle Zahlen ω eines endlichen Moduls $\mathfrak{o}$ durch Multiplication mit rationalen, von Null verschiedenen Zahlen in Zahlen eines Moduls $\mathfrak{m}$ verwandelt werden können, so enthält $\mathfrak{o}$ nur eine endliche Anzahl incongruenter Zahlen (mod. $\mathfrak{m}$).

Da es nämlich n rationale, von Null verschiedene Zahlen $r_1, r_2 \ldots r_n$ der Art giebt, dass die Producte $r_1\omega_1, r_2\omega_2 \ldots r_n\omega_n$ in $\mathfrak{m}$ enthalten sind, so giebt es auch eine ganze rationale, von Null verschiedene Zahl s der Art, dass alle Producte $s\omega \equiv 0$ (mod. $\mathfrak{m}$) sind. Lässt man daher jede der n ganzen rationalen Zahlen $h_1, h_2 \ldots h_n$ ein vollständiges Restsystem (mod. s) durchlaufen, so entstehen s^n Zahlen ω von der Form (1), und jede Zahl des Moduls $\mathfrak{o}$ ist wenigstens einer derselben congruent (mod. $\mathfrak{m}$); mithin ist die Anzahl der in $\mathfrak{o}$ enthaltenen, nach $\mathfrak{m}$ incongruenten Zahlen *höchstens* $= s^n$, was zu beweisen war.

Allein es ist wichtig, die Anzahl dieser incongruenten Zahlen *genau* zu bestimmen. Zu diesem Zweck betrachten wir das kleinste gemeinschaftliche Vielfache $\mathfrak{a}$ der beiden Moduln $\mathfrak{o}$ und $\mathfrak{m}$; da je zwei nach $\mathfrak{m}$ congruente Zahlen ω, ω' des Modul $\mathfrak{o}$ auch nach $\mathfrak{a}$ congruent sind, und umgekehrt, so ist unsere Aufgabe die, die Anzahl der Classen (mod. $\mathfrak{a}$) zu bestimmen, aus welchen $\mathfrak{o}$ besteht. Wir suchen daher zunächst die allgemeine Form aller in $\mathfrak{a}$ enthaltenen Zahlen

$$\alpha = k_1\omega_1 + k_2\omega_2 + \cdots + k_n\omega_n \quad (2)$$

aufzustellen, wo $k_1, k_2 \ldots k_n$ jedenfalls ganze rationale Zahlen bedeuten. Ist nun r ein bestimmter Index aus der Reihe $1, 2 \ldots n$, so giebt es unter allen den Zahlen $\alpha = \theta_r$, in welchen $k_{r+1} = 0$, $k_{r+2} = 0 \ldots k_n = 0$ ist, auch solche, in denen k_r von Null verschieden ist (z. B. $s\,\omega_r$), und unter diesen sei

$$\alpha_r = a_1^{(r)}\omega_1 + a_2^{(r)}\omega_2 + \cdots + a_r^{(r)}\omega_r \quad (3)$$

eine solche, in welcher k_r den *kleinsten* positiven Werth $a_r^{(r)}$ besitzt. Dann leuchtet ein, dass der Werth von k_r in jeder Zahl θ_r durch $a_r^{(r)}$ theilbar, also von der Form $a_r^{(r)}x_r$ ist, wo x_r eine ganze rationale Zahl bedeutet, und dass folglich $\theta_r - x_r\alpha_r = \theta_{r-1}$ eine Zahl α ist, in welcher $k_r, k_{r+1} \ldots k_n$ verschwinden. Hieraus folgt sofort, dass, nachdem man für jeden Index r eine solche particuläre Zahl α_r des Moduls $\mathfrak{a}$ aufgestellt hat*), jede Zahl α gewiss in die Form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \quad (4)$$

gebracht werden kann, wo $x_1, x_2 \ldots x_n$ ganze rationale Zahlen bedeuten, aus welchen die in der Form (2) vorkommenden Zahlen $k_1, k_2 \ldots k_n$ durch die Gleichungen

$$k_r = a_r^{(r)}x_r + a_r^{(r+1)}x_{r+1} + \cdots + a_r^{(n)}x_n \quad (5)$$

abgeleitet werden; und umgekehrt sind alle Zahlen α von der Form (4) in $\mathfrak{a}$ enthalten.

Ist nun eine Zahl ω von der Form (1) gegeben, sind also h_1, $h_2 \ldots h_n$ gegebene rationale ganze Zahlen, so sind *alle* Zahlen ω' des Moduls $\mathfrak{o}$, welche ihr nach $\mathfrak{m}$ congruent sind, welche also eine Classe (mod. $\mathfrak{a}$) bilden, von der Form

$$\omega' = \omega + \alpha = h_1'\omega_1 + h_2'\omega_2 + \cdots + h_n'\omega_n, \quad (6)$$

*) Das System dieser n particulären Zahlen wird ein vollständig bestimmtes, wenn man die Bedingung hinzufügt, dass $0 \leq a_r^{(r')} < a_r^{(r)}$ sein soll, wenn $r' > r$ ist.

wo zufolge (5)

$$h'_r = h_r + a_r^{(r)} x_r + a_r^{(r+1)} x_{r+1} + \cdots + a_r^{(n)} x_n$$

ist, und hieraus folgt, dass man successive die willkürlichen rationalen ganzen Zahlen $x_n, x_{n-1} \ldots x_2, x_1$ stets und nur auf eine einzige Art so bestimmen kann, dass die n Zahlen h'_r den Bedingungen

$$0 \leqq h'_r < a_r^{(r)} \tag{7}$$

genügen. In jeder Classe existirt daher ein und nur ein *Repräsentant* ω' von der Form (6), welcher diesen Bedingungen (7) genügt; mithin ist die *Anzahl* der verschiedenen Classen (mod. $\mathfrak{a}$), aus welchen der Modul $\mathfrak{o}$ besteht, gleich dem Producte $a'_1 a''_2 \ldots a_n^{(n)}$, d. h. gleich der *Determinante* des Coefficientensystems in den n particulären Zahlen α_r von der Form (3), welche eine Basis von $\mathfrak{a}$ bilden *).

§. 162.

Wir beschränken uns von jetzt an auf die Untersuchung der ganzen Zahlen, welche in einem endlichen Körper Ω (§. 159) enthalten sind.

1. Da jede algebraische Zahl (zufolge §. 160, 5.) durch Multiplication mit einer rationalen ganzen von Null verschiedenen Zahl in eine ganze Zahl verwandelt werden kann, so dürfen wir annehmen, dass die Zahlen $\omega_1, \omega_2 \ldots \omega_n$, welche eine Basis des Körpers Ω bilden, sämmtlich *ganze* Zahlen sind, und es wird dann (zufolge §. 160, 1.) jede Zahl

$$\omega = \sum h_\iota \omega_\iota \tag{1}$$

gewiss eine ganze Zahl sein, wenn ihre Coordinaten h_ι rationale ganze Zahlen sind; aber dies lässt sich im Allgemeinen nicht umkehren, d. h. es kann ω sehr wohl eine ganze Zahl sein, auch wenn ihre Coordinaten theilweise oder sämmtlich gebrochene Zahlen

*) Die weitere Entwicklung der allgemeinen Theorie der Moduln würde uns hier zu weit führen (vergl. §. 163); wir erwähnen nur noch folgenden Satz: Sind die Basiszahlen eines endlichen Moduls von einander abhängig, so giebt es immer eine aus unabhängigen Zahlen bestehende Basis desselben Moduls. Die eleganteste Methode, die neue Basis aufzufinden, besteht in einer Verallgemeinerung der von *Gauss* angewandten Behandlung der partialen Determinanten (*D. A.* artt. 234, 236, 279).

sind. Dies ist einer der wichtigsten Puncte der Theorie und muss deshalb vor Allem aufgeklärt werden.

Wir schicken zunächst die einleuchtende Bemerkung voraus, dass die Discriminante (§. 159, (10)) eines jeden Systems von n unabhängigen ganzen Zahlen gewiss eine von Null verschiedene rationale und zwar *ganze* Zahl ist, weil sie durch Addition, Subtraction und Multiplication aus lauter ganzen Zahlen gebildet ist. Giebt es nun wirklich in Ω eine *ganze* Zahl

$$\beta = \frac{\sum k_\iota \omega_\iota}{s} \tag{2}$$

wo $s, k_1, k_2 \ldots k_n$ ganze rationale Zahlen ohne gemeinschaftlichen Theiler bedeuten, deren erste $s > 1$ ist, so behaupten wir, dass s^2 in der Discriminante $\Delta(\omega_1, \omega_2 \ldots \omega_n)$ aufgeht, und dass man eine neue Basis von ganzen Zahlen $\beta_1, \beta_2 \ldots \beta_n$ aufstellen kann, deren Discriminante absolut genommen $< \Delta(\omega_1, \omega_2 \ldots \omega_n)$ ist.

Um dies zu beweisen, bezeichnen wir mit $\mathfrak{m}$ den aus allen durch s theilbaren ganzen Zahlen bestehenden Modul, ebenso mit $\mathfrak{o}$ das System aller Zahlen ω von der Form (1), deren Coordinaten h_ι *ganze* Zahlen sind; da jedes Product $s\omega$ eine Zahl des Moduls $\mathfrak{m}$ ist, so können wir die allgemeine Untersuchung des vorigen Paragraphen auf unsern Fall anwenden. Alle durch s theilbaren Zahlen α des Systems $\mathfrak{o}$ sind daher von der Form

$$\alpha = \sum x_\iota \alpha_\iota = s \sum x_\iota \beta_\iota,$$

wo die n Zahlen $\alpha_\iota = s\beta_\iota$ particuläre Zahlen α, also die β_ι *ganze* Zahlen des Körpers Ω, und die x_ι willkürliche rationale ganze Zahlen bedeuten.

Da nun alle Zahlen $s\omega$ auch solche Zahlen α sind, so kann man

$$\omega_r = \sum b_\iota^{(r)} \beta_\iota, \quad \Delta(\omega_1, \omega_2 \ldots \omega_n) = b^2 \Delta(\beta_1, \beta_2 \ldots \beta_n)$$

setzen, wo die Coefficienten $b_\iota^{(r)}$ rationale ganze Zahlen sind, und b die aus ihnen gebildete Determinante bedeutet; durch Umkehrung ergiebt sich, dass die n Producte $b\beta_\iota$, mithin auch alle Quotienten $b\alpha : s$ *Zahlen des Systems* $\mathfrak{o}$ sind.

Wenden wir dies Resultat auf die obige Voraussetzung (2) an, dass die Zahl β eine ganze Zahl, ihr Zähler $\sum k_\iota \omega_\iota$ also eine Zahl α ist, obgleich die Zahlen $s, k_1, k_2 \ldots k_n$ keinen gemeinschaftlichen Theiler haben, so folgt unmittelbar, dass b *durch* s *theilbar* ist, wodurch zugleich die obigen Behauptungen erwiesen sind.

Da nun die Discriminante eines jeden Systems von n unabhängigen ganzen Zahlen des Körpers Ω eine von Null verschiedene ganze rationale Zahl ist, so giebt es unter allen diesen Discriminanten eine solche, deren Werth — abgesehen vom Vorzeichen — ein *Minimum* ist, und aus der vorstehenden Untersuchung folgt unmittelbar, dass, wenn eine Basis aus solchen ganzen Zahlen $\omega_1, \omega_2 \ldots \omega_n$ besteht, deren Discriminante diesen Minimumwerth besitzt, die entsprechenden Coordinaten h_ι einer jeden *ganzen* Zahl ω des Körpers nothwendig *ganze* rationale Zahlen sein müssen. Eine solche Basis $\omega_1, \omega_2 \ldots \omega_n$ wollen wir eine *Grundreihe* des Körpers Ω nennen; aus ihr ergeben sich alle anderen Grundreihen desselben Körpers, wenn man n ganze Zahlen ω von der Form (1) so wählt, dass die aus den n^2 zugehörigen Coordinaten gebildete Determinante $= \pm 1$ wird.

Die wichtigste Rolle spielt aber die Minimaldiscriminante selbst, sowohl hinsichtlich der inneren*) Constitution des Körpers Ω, als auch hinsichtlich seiner Verwandtschaft mit anderen Körpern**); wir wollen daher diese positive oder negative ganze rationale Zahl die *Grundzahl* oder die *Discriminante des Körpers* Ω nennen und mit $\Delta(\Omega)$ bezeichnen; sie ist offenbar zugleich die Grundzahl eines jeden mit Ω conjugirten Körpers.

Die Zahlen eines quadratischen Körpers sind z. B. von der Form $t + u\sqrt{D}$, wo t, u alle rationalen Zahlen durchlaufen, und D eine ganze rationale Zahl bedeutet, welche kein Quadrat und auch durch kein Quadrat ausser 1 theilbar ist. Ist $D \equiv 1 \pmod{4}$, so bilden die Zahlen 1 und $\frac{1}{2}(1 + \sqrt{D})$ eine Grundreihe des Körpers, und seine Grundzahl ist $= D$; ist dagegen $D \equiv 2$ oder $\equiv 3 \pmod{4}$, so bilden die Zahlen 1 und $\sqrt{D}$ eine Grundreihe des Körpers, und seine Grundzahl ist $= 4D$.

*) Vergl. *Kronecker: Ueber die algebraisch auflösbaren Gleichungen* (Monatsbericht der Berliner Ak. 14. April 1856).

**) Die erste Spur dieser Beziehungen hat sich bei einer schönen Untersuchung von *Kronecker* gezeigt (*Mémoire sur les facteurs irréductibles de l'expression* $x^n - 1$; Journ. de Math., p. p. Liouville; T. XIX. 1854). Um den Charakter dieser Gesetze, deren Entwicklung ich mir auf eine andere Gelegenheit verspare, näher anzudeuten, führe ich nur das einfachste Beispiel an: das kleinste gemeinschaftliche Multiplum zweier von einander verschiedenen quadratischen Körper A, B ist ein biquadratischer Körper K, der noch einen dritten quadratischen Körper C zum Divisor hat; die Grundzahl von K ist gleich dem Product aus den Grundzahlen von A, B, C, und zwar eine Quadratzahl.

Ist ferner θ eine primitive Wurzel der Gleichung $\theta^m = 1$ (§. 139), wo $m > 2$, so bilden die Zahlen $1, \theta, \theta^2 \ldots \theta^{n-1}$ die Grundreihe eines Körpers vom Grade $n = \varphi(m)$, dessen Grundzahl

$$\left(\frac{m\sqrt{-1}}{\sqrt[a-1]{a}\,\sqrt[b-1]{b}\,\sqrt[c-1]{c}\ldots}\right)^n$$

ist, wo $a, b, c \ldots$ alle verschiedenen in m aufgehenden Primzahlen bedeuten. Ist $m = 3$ (oder $= 6$), so ist dieser Körper ein quadratischer, seine Grundzahl $= -3$; ist $m = 4$, so ist die Grundzahl des quadratischen Körpers $= -4$.

2. Aus den vorstehenden Principien ergiebt sich leicht der folgende Fundamentalsatz:

Ist μ eine von Null verschiedene ganze Zahl des Körpers Ω, so ist die Anzahl der nach dem Modul μ incongruenten ganzen Zahlen des Körpers gleich dem absoluten Werth der Norm des Moduls μ.

Es sei $\mathfrak{m}$ das System aller durch μ theilbaren ganzen Zahlen (welche sich durch Addition und Subtraction reproduciren), und $\mathfrak{o}$ das System *aller* ganzen Zahlen des Körpers Ω, d. h. aller Zahlen ω von der Form (1), wo die Zahlen ω_ι eine *Grundreihe* des Körpers bilden, und die Coordinaten h_ι beliebige ganze rationale Zahlen bedeuten; da jeder Quotient $\omega : \mu$ (zufolge §. 160, 5.) durch Multiplication mit einer von Null verschiedenen ganzen rationalen Zahl in eine ganze Zahl verwandelt werden kann, so ist die Untersuchung des vorigen Paragraphen auf unsern Fall anwendbar. Mithin sind alle durch μ theilbaren Zahlen α des Systems $\mathfrak{o}$ von der Form

$$\alpha = \sum x_\iota \alpha_\iota = \mu \sum x_\iota \beta_\iota,$$

wo die n Zahlen $\alpha_\iota = \mu\beta_\iota$ particuläre Zahlen α bedeuten, also die Zahlen β_ι in $\mathfrak{o}$ enthalten sind, und die Grössen x_ι alle rationalen ganzen Zahlwerthe annehmen dürfen; die Anzahl der *Classen*, in welche das System $\mathfrak{o}$ in Bezug auf den Modul μ zerfällt, ist ferner gleich der aus den Coordinaten der n Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ gebildeten Determinante a. Zugleich ist (nach §. 159, (11), (12))

$$\Delta(\alpha_1 \ldots \alpha_n) = a^2 \Delta(\Omega) = N(\mu)^2 \Delta(\beta_1 \ldots \beta_n);$$

da nun jede durch μ theilbare Zahl $\alpha = \mu\omega$ des Systems $\mathfrak{o}$ die Form $\mu \sum x_\iota \beta_\iota$ besitzt, so ist jede Zahl ω des Systems $\mathfrak{o}$ auch von der Form $\sum x_\iota \beta_\iota$; mithin bilden die Zahlen β_ι ebenfalls eine *Grund-*

reihe des Körpers, und folglich ist $\Delta(\beta_1 \ldots \beta_n) = \Delta(\Omega)$, also $a = \pm N(\mu)$, was zu beweisen war.

Zugleich leuchtet ein, dass nach der Methode des vorigen Paragraphen ein System von a incongruenten Repräsentanten der verschiedenen Classen, also ein *vollständiges Restsystem für den Modul* μ aufgestellt werden kann*).

3. Will man jetzt zwei gegebene ganze Zahlen θ, μ darauf prüfen, ob sie relative Primzahlen sind, so braucht man offenbar ω nur ein vollständiges Restsystem (mod. μ) durchlaufen zu lassen und nachzusehen, wie oft $\theta\omega \equiv 0$ (mod. μ) wird; zeigt sich, dass dies nur dann eintritt, wenn $\omega \equiv 0$ (mod. μ) ist, so ist also jede durch θ und μ theilbare ganze Zahl $\theta\omega$ auch theilbar durch $\theta\mu$, mithin sind θ, μ relative Primzahlen; besitzt aber die Congruenz $\theta\omega \equiv 0$ (mod. μ) auch eine Wurzel ω, welche nicht $\equiv 0$ (mod. μ) ist, so ist die entsprechende Zahl $\theta\omega$ durch θ und μ, aber nicht durch $\theta\mu$ theilbar, mithin sind θ, μ keine relative Primzahlen.

Ist θ relative Primzahl zu μ (z. B. $\theta = 1$), so durchläuft $\theta\omega$ gleichzeitig mit ω ein vollständiges Restsystem (mod. μ); folglich hat jede Congruenz $\theta\omega \equiv \theta'$ (mod. μ) immer eine und nur eine Wurzel ω (vergl. §. 22); ist ferner $\psi(\mu)$ die Anzahl aller Classen, deren Zahlen relative Primzahlen zum Modul μ sind, so durchläuft $\theta\omega$ gleichzeitig mit ω die Repräsentanten aller dieser Classen, und da das Product dieser Zahlen ω auch relative Primzahl zu μ ist, so ergiebt sich der Satz

$$\theta^{\psi(\mu)} \equiv 1 \text{ (mod. } \mu),$$

welcher dem Fermat'schen Satze (§. 19) entspricht.

4. Verfolgt man diese Analogie mit der rationalen Zahlentheorie weiter, so drängt sich immer wieder die Frage nach der Zusammensetzung der Zahlen des Systems $\mathfrak{o}$ (d. h. der ganzen Zahlen des Körpers Ω) aus Factoren auf, welche demselben System $\mathfrak{o}$ an-

*) Bilden die n Zahlen ω_ι *irgend* eine Basis des Körpers Ω, und ist $\mathfrak{o}$ das System aller der Zahlen ω von der Form (1), deren Coordinaten *ganze* Zahlen sind, so reproduciren sich die Zahlen des Systems $\mathfrak{o}$ durch Addition und Subtraction; nimmt man ferner an, dass sie sich auch durch Multiplication reproduciren, woraus zugleich folgt, dass sie *ganze* Zahlen sind, und nennt man zwei solche Zahlen ω, ω' stets und nur dann congruent in Bezug auf eine dritte solche Zahl μ, wenn der Quotient $(\omega - \omega') : \mu$ wieder eine Zahl des Systems $\mathfrak{o}$ ist, so ist die Anzahl der in $\mathfrak{o}$ enthaltenen, nach μ incongruenten Zahlen ebenfalls $= \pm N(\mu)$. Vergl. §. 165, 4.

gehören, und es zeigt sich zunächst, dass die unbegrenzte Zerlegbarkeit der ganzen Zahlen, wie sie in dem unendlichen Körper *aller* algebraischen Zahlen auftrat (§. 160, 7.), in einem endlichen Körper Ω wieder verschwindet. Dafür tritt aber bei unendlich vielen solchen Körpern Ω ein höchst eigenthümliches Phänomen auf, das schon früher (§. 16) gelegentlich erwähnt ist*). Nennt man eine Zahl in $\mathfrak{o}$ *zerlegbar*, wenn sie das Product aus zwei Zahlen in $\mathfrak{o}$ ist, welche beide keine Einheiten sind, dagegen *unzerlegbar*, wenn dies nicht der Fall ist, so ist offenbar jede zerlegbare Zahl μ darstellbar als Product aus einer *endlichen* Anzahl von unzerlegbaren Zahlen (vergl. §. 8), weil die Norm von μ gleich dem Producte aus den Normen der einzelnen Factoren ist (§. 159); aber es zeigt sich häufig, dass diese Zerlegung nicht eine vollkommen bestimmte ist, sondern dass mehrere *wesentlich verschiedene* Zerlegungen derselben Zahl in unzerlegbare Factoren existiren (§. 160, 6.). Dies widerspricht so sehr dem in der rationalen Zahlentheorie herrschenden Begriffe des Primzahlcharakters (§. 8), dass wir deshalb eine unzerlegbare Zahl als solche noch nicht als Primzahl anerkennen wollen; wir suchen daher für den wahren Primzahlcharakter ein kräftigeres Kriterium als diese unzulängliche Unzerlegbarkeit aufzustellen, ähnlich wie früher bei dem Begriffe der relativen Primzahl (§. 160, 7.), indem wir die zu untersuchende Zahl μ nicht zerlegen, sondern ihr Verhalten als *Modul* betrachten:

Eine ganze Zahl μ, welche keine Einheit ist, soll eine Primzahl heissen, wenn jedes durch μ theilbare Product $\eta\varrho$ wenigstens einen durch μ theilbaren Factor η oder ϱ besitzt.

Es ergiebt sich dann sofort, dass die höchste in einem Producte aufgehende Potenz einer Primzahl μ das Product aus den höchsten in den einzelnen Factoren aufgehenden Potenzen von μ,

---

*) Das dortige Beispiel passt freilich nicht ganz hierher, insofern die ganzen Zahlen des der Gleichung $\varrho^2 = -11$ entsprechenden quadratischen Körpers nicht durch die Form $t + u\varrho$, wohl aber durch die Form $t + u\theta$ erschöpft werden, wo $2\theta = 1 + \varrho$ ist; die Zahlen $3, 5, 2 + \varrho, 2 - \varrho$ sind in der That zerlegbar: $3 = \theta(1-\theta)$, $5 = (1+\theta)(2-\theta)$, $2 - \varrho = -\theta(1+\theta)$, $2 + \varrho = -(1-\theta)(2-\theta)$; die vier Zahlen $\theta, 1-\theta, 1+\theta, 2-\theta$ sind Primzahlen in diesem Körper. Die in Rede stehende Erscheinung tritt aber in dem der Gleichung $x^2 = -5$ entsprechenden quadratischen Körper an dem Beispiel $3 . 7 = (1+2x)(1-2x)$ wirklich auf (vergl. §. 71; die beiden Zahlen 3, 7 sind durch die Hauptform der Determinante -5 nicht darstellbar).

und dass jede durch μ nicht theilbare Zahl relative Primzahl zu μ ist. Man erkennt ferner leicht, dass die kleinste durch μ theilbare rationale ganze Zahl p nothwendig eine Primzahl (im Körper der rationalen Zahlen), und folglich die Norm von μ eine Potenz von p, nämlich ein rationaler Divisor von $N(p) = p^n$ sein muss. Es werden daher gewiss alle Primzahlen μ des Körpers Ω entdeckt, wenn die Divisoren aller rationalen Primzahlen p aufgesucht werden.

5. Ist aber μ keine Primzahl (und auch keine Einheit), existiren also zwei durch μ nicht theilbare Zahlen η, ϱ, deren Product $\eta\varrho$ durch μ theilbar ist, so schreiten wir zu einer Zerlegung von μ in wirkliche oder *ideale*, d. h. fingirte Factoren. Giebt es nämlich in $\mathfrak{o}$ einen grössten gemeinschaftlichen Theiler ν der beiden Zahlen η und $\mu = \nu\mu'$, der Art, dass die Quotienten $\eta:\nu$ und $\mu:\nu$ relative Primzahlen sind, so ist μ in die beiden Factoren ν und μ' zerlegt, von denen keiner eine Einheit ist, weil weder ϱ noch η durch μ theilbar ist. Der Factor μ' ist wesentlich dadurch bestimmt, dass alle Wurzeln α' der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ durch μ' theilbar sind (z. B. auch $\alpha' = \varrho$), und dass ebenso jede durch μ' theilbare Zahl α' auch der vorstehenden Congruenz genügt. Umgekehrt, giebt es in $\mathfrak{o}$ eine Zahl μ', welche in allen Wurzeln α' der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ und nur in diesen aufgeht, so ist auch μ theilbar durch μ', und der Quotient $\nu = \mu:\mu'$ ist der grösste gemeinschaftliche Theiler der beiden Zahlen η und μ.

Aber es kann sehr wohl der Fall eintreten, dass in $\mathfrak{o}$ keine solche Zahl μ' zu finden ist; als nun diese Erscheinung (bei den aus Einheitswurzeln gebildeten Zahlen) *Kummer* entgegentrat, so kam er auf den glücklichen Gedanken, trotzdem eine solche Zahl μ' zu fingiren und dieselbe als *ideale Zahl* einzuführen; die *Theilbarkeit* einer Zahl α' durch diese ideale Zahl μ' besteht lediglich darin, dass α' eine Wurzel der Congruenz $\eta\alpha' \equiv 0 \pmod{\mu}$ ist, und da diese idealen Zahlen in der Folge immer nur als Theiler oder Moduln auftreten, so hat diese Art ihrer Einführung durchaus keine Bedenken. Allein die Befürchtung, dass die unmittelbare Uebertragung der bei den *wirklichen* Zahlen üblichen Benennungen auf die idealen Zahlen im Anfang leicht Misstrauen gegen die Sicherheit der Beweisführung einflössen könnte, veranlasst uns, die Untersuchung dadurch in ein anderes Gewand einzukleiden, dass wir immer ganze *Systeme* von wirklichen Zahlen betrachten.

§. 163.

Wir gründen die Theorie der in $\mathfrak{o}$ enthaltenen Zahlen, d. h. aller ganzen Zahlen des Körpers Ω, auf den folgenden neuen Begriff.

1. Ein System $\mathfrak{a}$ von unendlich vielen in $\mathfrak{o}$ enthaltenen Zahlen soll ein *Ideal* heissen, wenn es den beiden Bedingungen genügt:

I. Die Summe und die Differenz je zweier Zahlen in $\mathfrak{a}$ sind wieder Zahlen in $\mathfrak{a}$.

II. Jedes Product aus einer Zahl in $\mathfrak{a}$ und einer Zahl in $\mathfrak{o}$ ist wieder eine Zahl in $\mathfrak{a}$.

Ist α in $\mathfrak{a}$ enthalten, so sagen wir, α sei *theilbar durch* $\mathfrak{a}$, $\mathfrak{a}$ *gehe in* α *auf*, weil die Ausdrucksweise hierdurch an Leichtigkeit gewinnt. Wir nennen ferner zwei in $\mathfrak{o}$ enthaltene Zahlen ω, ω', deren Differenz durch $\mathfrak{a}$ theilbar ist, *congruent nach* $\mathfrak{a}$ (vergl. §. 161), und bezeichnen dies durch die Congruenz $\omega \equiv \omega' \pmod{\mathfrak{a}}$; solche Congruenzen dürfen (zufolge I.) addirt, subtrahirt und (zufolge II.) multiplicirt werden, wie Gleichungen. Da je zwei einer dritten congruente Zahlen auch einander congruent sind, so kann man alle Zahlen in *Classen* (mod. $\mathfrak{a}$) eintheilen, indem man je zwei congruente Zahlen in dieselbe, je zwei incongruente Zahlen in zwei verschiedene Classen wirft; da nun, wenn μ eine von Null verschiedene Zahl in $\mathfrak{a}$ bedeutet, je zwei nach μ congruente Zahlen (zufolge II.) auch nach $\mathfrak{a}$ congruent sind — woraus zugleich folgt, dass $\mathfrak{a}$ aus einer oder mehreren Classen (mod. μ) besteht — so ist (zufolge §. 162, 2.) die Anzahl der Classen (mod. $\mathfrak{a}$), in welche $\mathfrak{o}$ zerfällt, *endlich**). Wählt man aus jeder Classe ein Individuum als Repräsentanten, so bilden dieselben ein *vollständiges Restsystem* (mod. $\mathfrak{a}$); die Anzahl dieser Classen oder incongruenten Zahlen soll die *Norm* von $\mathfrak{a}$ heissen und mit $N(\mathfrak{a})$ bezeichnet werden.

Ist η eine von Null verschiedene Zahl in $\mathfrak{o}$, so bilden alle durch η theilbaren Zahlen in $\mathfrak{o}$ ein Ideal, welches mit $\mathfrak{i}(\eta)$ bezeichnet werden soll; solche Ideale sind besonders ausgezeichnet und sollen

---

*) Dasselbe ergiebt sich unmittelbar aus §. 161; ist nämlich ω irgend eine Zahl in $\mathfrak{o}$, so kann durch Multiplication mit einer von Null verschiedenen ganzen rationalen Zahl der Quotient $\omega : \mu$ in eine ganze Zahl, also ω (zufolge II.) in eine Zahl des Ideals $\mathfrak{a}$ verwandelt werden.

Hauptideale heissen; die Norm von $\mathfrak{i}(\eta)$ ist $= \pm N(\eta)$; ist η eine Einheit, so ist $\mathfrak{i}(\eta) = \mathfrak{o}$, und umgekehrt.

2. Wenn alle Zahlen eines Ideals $\mathfrak{a}$ auch in einem Ideal $\mathfrak{b}$ enthalten sind, so besteht offenbar $\mathfrak{b}$ aus einer oder mehreren Classen (mod. $\mathfrak{a}$), und wir wollen sagen, $\mathfrak{a}$ sei ein *Multiplum von* $\mathfrak{b}$ oder *theilbar durch* $\mathfrak{b}$, $\mathfrak{b}$ sei ein *Theiler von* $\mathfrak{a}$ oder *gehe in* $\mathfrak{a}$ *auf*.

Besteht $\mathfrak{b}$ aus r Classen (mod. $\mathfrak{a}$), so ist $N(\mathfrak{a}) = rN(\mathfrak{b})$. Durchläuft nämlich δ die Repräsentanten dieser r Classen, und γ ein vollständiges Restsystem (mod. $\mathfrak{b}$), so bilden die $rN(\mathfrak{b})$ Zahlen $\gamma + \delta$ ein vollständiges Restsystem (mod. $\mathfrak{a}$); denn erstens ist jede Zahl in $\mathfrak{o}$ congruent einer Zahl γ (mod. $\mathfrak{b}$), also $\equiv \gamma + \delta$ (mod. $\mathfrak{a}$), und zweitens folgt aus $\gamma + \delta \equiv \gamma' + \delta'$ (mod. $\mathfrak{a}$), wo γ', δ' ähnliche Bedeutung haben wie γ, δ, successive $\gamma + \delta \equiv \gamma' + \delta'$ (mod. $\mathfrak{b}$), $\gamma \equiv \gamma'$ (mod. $\mathfrak{b}$), $\gamma = \gamma'$, also $\delta \equiv \delta'$ (mod. $\mathfrak{a}$), $\delta = \delta'$, d. h. die sämmtlichen Zahlen $\gamma + \delta$ sind incongruent (mod. $\mathfrak{a}$).

Ein Ideal besitzt folglich nur eine *endliche* Anzahl von Theilern. Ist $\mathfrak{m}$ theilbar durch $\mathfrak{a}$, $\mathfrak{a}$ durch $\mathfrak{b}$, so ist auch $\mathfrak{m}$ durch $\mathfrak{b}$ theilbar. Das Hauptideal $\mathfrak{o}$ selbst geht in jedem Ideal auf und ist zugleich das *einzige* Ideal, welches die Zahl 1 oder überhaupt Einheiten enthält, und dessen Norm $= 1$ ist.

Das System aller derjenigen Zahlen, welche gleichzeitig in zwei Idealen $\mathfrak{a}$, $\mathfrak{b}$ enthalten sind, ist das *kleinste gemeinschaftliche Multiplum* $\mathfrak{m}$ von $\mathfrak{a}$, $\mathfrak{b}$, insofern jedes gemeinschaftliche Multiplum von $\mathfrak{a}$, $\mathfrak{b}$ durch das Ideal $\mathfrak{m}$ theilbar ist. Durchläuft α alle Zahlen in $\mathfrak{a}$, β alle Zahlen in $\mathfrak{b}$, so ist das System aller Zahlen $\alpha + \beta$ der *grösste gemeinschaftliche Theiler* $\mathfrak{d}$ der Ideale $\mathfrak{a}$, $\mathfrak{b}$, weil jeder gemeinschaftliche Theiler von $\mathfrak{a}$, $\mathfrak{b}$ in dem Ideale $\mathfrak{d}$ aufgeht*).

Ist r die Anzahl der in $\mathfrak{b}$ enthaltenen Zahlen, welche (mod. $\mathfrak{a}$) incongruent sind, so besteht $\mathfrak{b}$ aus r Classen (mod. $\mathfrak{m}$), und $\mathfrak{d}$ aus r Classen (mod. $\mathfrak{a}$); also ist $N(\mathfrak{m}) = rN(\mathfrak{b})$, $N(\mathfrak{a}) = rN(\mathfrak{d})$, und $N(\mathfrak{m})N(\mathfrak{d}) = N(\mathfrak{a})N(\mathfrak{b})$.

Ist $\mathfrak{b}$ ein Hauptideal $= \mathfrak{i}(\eta)$, so ist die Anzahl r der in $\mathfrak{b}$ enthaltenen Zahlen $\beta = \eta\omega$, welche (mod. $\mathfrak{a}$) incongruent sind, zugleich die Norm des aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{a}$) bestehenden Ideals $\mathfrak{r}$, weil zwei Zahlen ω, ω' stets und nur dann congruent (mod. $\mathfrak{r}$) sind, wenn $\eta\omega \equiv \eta\omega'$ (mod $\mathfrak{a}$) ist. Mithin ist in diesem Falle $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{b})$.

*) Die Erweiterung dieser Definitionen von $\mathfrak{m}$ und $\mathfrak{d}$ für mehr als zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ . . . liegt auf der Hand.

3. Ein von $\mathfrak{o}$ verschiedenes Ideal $\mathfrak{p}$, welches keinen von $\mathfrak{o}$ und $\mathfrak{p}$ verschiedenen Theiler besitzt, soll ein *Primideal* heissen. Dann gilt folgender Satz:

Ist $\eta\varrho \equiv 0$ *(mod.* $\mathfrak{p}$*), so ist wenigstens eine der beiden Zahlen* η, ϱ *durch* $\mathfrak{p}$ *theilbar.* Ist nämlich η nicht $\equiv 0$ (mod. $\mathfrak{p}$), so bilden die sämmtlichen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{p}$) offenbar ein in $\mathfrak{p}$ aufgehendes Ideal, welches, da es die Zahl 1 nicht enthält, von $\mathfrak{o}$ verschieden und folglich mit $\mathfrak{p}$ identisch ist, was zu beweisen war.

Dieser Satz ist charakteristisch für ein Primideal, da er sich folgendermaassen umkehren lässt: *Enthält jedes durch ein (von* $\mathfrak{o}$ *verschiedenes) Ideal* $\mathfrak{p}$ *theilbare Product mindestens einen durch* $\mathfrak{p}$ *theilbaren Factor, so ist* $\mathfrak{p}$ *ein Primideal.* Ist nämlich $\mathfrak{q}$ ein Theiler des Ideals $\mathfrak{p}$, aber verschieden von $\mathfrak{p}$, so giebt es in $\mathfrak{q}$ eine nicht in $\mathfrak{p}$ enthaltene Zahl ω; dann ist (zufolge der Annahme) auch keine der Potenzen $\omega^2, \omega^3 \ldots$ durch $\mathfrak{p}$ theilbar; da aber nur eine endliche Anzahl von incongruenten Zahlen (mod. $\mathfrak{p}$) existirt, so muss einmal für zwei *verschiedene* Exponenten m und $m + s > m$ nothwendig $\omega^{m+s} \equiv \omega^m$ (mod. $\mathfrak{p}$), also das Product $\omega^m(\omega^s - 1)$ durch $\mathfrak{p}$ theilbar sein; da nun ω^m nicht durch $\mathfrak{p}$ theilbar ist, so muss (zufolge der Annahme) der andere Factor $\omega^s - 1$ durch $\mathfrak{p}$, und folglich auch durch $\mathfrak{q}$ theilbar sein; nun ist ω und, weil $s > 0$ ist, auch $\omega^s \equiv 0$ (mod. $\mathfrak{q}$), mithin ist auch die Zahl 1 in $\mathfrak{q}$ enthalten, also $\mathfrak{q} = \mathfrak{o}$, was zu beweisen war.

Nennt man ein von $\mathfrak{o}$ verschiedenes Ideal *zusammengesetzt*, wenn es kein Primideal ist, so lässt sich dieser Satz auch so aussprechen: *Ist* $\mathfrak{a}$ *ein zusammengesetztes Ideal, so giebt es zwei durch* $\mathfrak{a}$ *nicht theilbare Zahlen* η, ϱ, *deren Product* $\eta\varrho$ *durch* $\mathfrak{a}$ *theilbar ist.* Wir beweisen ihn zum zweiten Male auf folgende Art. Es sei $\mathfrak{e}$ ein von $\mathfrak{a}$ und $\mathfrak{o}$ verschiedener Theiler von $\mathfrak{a}$, so giebt es in $\mathfrak{e}$ eine durch $\mathfrak{a}$ nicht theilbare Zahl η, und der grösste gemeinschaftliche Theiler $\mathfrak{d}$ von $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ ist theilbar durch $\mathfrak{e}$, also von $\mathfrak{o}$ verschieden, mithin ist $N(\mathfrak{d}) > 1$. Das aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{a}$) bestehende Ideal $\mathfrak{r}$ ist ein Theiler von $\mathfrak{a}$, und da (zufolge 2.) $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d}) > N(\mathfrak{r})$ ist, so ist $\mathfrak{r}$ verschieden von $\mathfrak{a}$ und enthält folglich eine durch $\mathfrak{a}$ nicht theilbare Zahl ϱ, was zu beweisen war.

Es leuchtet nun ein, dass die kleinste (von Null verschiedene) rationale Zahl p, welche in einem Primideale $\mathfrak{p}$ enthalten ist, nothwendig eine *Primzahl* (im rationalen Zahlkörper) sein muss; da

ferner $\mathfrak{p}$ in $\mathfrak{i}(p)$ aufgeht, so ist $N(\mathfrak{p})$ ein Theiler von $N(p) = p^n$, also ebenfalls eine Potenz p^f der rationalen Primzahl p, und man findet leicht (vergl. §. 162, 3.), dass jede in $\mathfrak{o}$ enthaltene Zahl ω der Congruenz

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}}$$

genügt*). Auch hat es keine Schwierigkeit, die allgemeinen Sätze der §§. 26, 27, 29, 30, 31 auf Congruenzen in Bezug auf den Modul $\mathfrak{p}$ zu übertragen.

Ist das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ *der Ideale* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ *durch das Primideal* $\mathfrak{p}$ *theilbar, so geht* $\mathfrak{p}$ *wenigstens in einem der Ideale* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ *auf.* Ist nämlich *keins* dieser Ideale durch $\mathfrak{p}$ theilbar, giebt es also in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$ resp. Zahlen $\alpha, \beta, \gamma \ldots$, die nicht durch $\mathfrak{p}$ theilbar sind, so ist das in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \ldots$, also auch in

*) Hierauf beruht das Eingreifen der *Theorie der höheren Congruenzen* (vergl. §. 26), welche zur Bestimmung der Primideale dient. Für die Körper vom Grade $n = \varphi(m)$, welche aus den primitiven Wurzeln θ der Gleichung $\theta^m = 1$ entspringen, ist dieselbe zuerst ausgeführt, und zwar von *Kummer*, dem Schöpfer der Theorie der idealen Zahlen; den hierauf bezüglichen Theil seiner Untersuchungen findet man am vollständigsten zusammengestellt in den Abhandlungen: *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers* (Journ. de Math. p. p. Liouville, T. XVI. 1851). — *Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn* n *eine zusammengesetzte Zahl ist* (Abh. der Berliner Ak. 1856). Das Hauptresultat ergiebt sich mit grösster Leichtigkeit aus unserer Theorie und lautet in unserer Ausdrucksweise folgendermassen: Ist p eine rationale Primzahl und m' der grösste durch p nicht theilbare Divisor von $m = p'm'$, gehört ferner p zum Exponenten f (mod. m'), wo $\varphi(m') = ef$ (§. 28), so ist $\mathfrak{i}(p) = (\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_e)^{\varphi(p')}$, wo $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_e$ von einander verschiedene Primideale bedeuten, deren Normen $= p^f$ sind; wenn $p' > 1$, so ist $\mathfrak{i}(1 - \theta^{m'}) = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_e$. — Für complexe Zahlen einer höheren Stufe vergl. *Kummer: Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist* (Abh. der Berliner Ak. 1859). — Für diejenigen Körper Ω, deren conjugirte Körper mit Ω identisch sind, und welche ich *Galois'sche Körper* nennen möchte, vergl. *Selling: Ueber die idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln einer beliebigen irreductibelen Gleichung rational gebildet sind* (Schlömilch's Zeitschr. für Math. u. Phys. Bd. 10. 1865). — Ein specieller Fall biquadratischer Körper ist vollständig durchgeführt von *Bachmann: Die Theorie der complexen Zahlen, welche aus zwei Quadratwurzeln zusammengesetzt sind.* 1867. — Für eine gewisse Classe cubischer Körper vergl. *Eisenstein: Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreistheilung ihre Entstehung verdanken* (Crelle's Journ. XXVIII).

$\mathfrak{m}$ enthaltene Product $\alpha\beta\gamma\ldots$ nicht theilbar durch das Primideal $\mathfrak{p}$, und folglich geht $\mathfrak{p}$ *nicht* in $\mathfrak{m}$ auf, was zu beweisen war.

Ist die Zahl η nicht theilbar durch das Ideal $\mathfrak{a}$, so giebt es immer eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. $\mathfrak{a}$) ein Primideal bilden. Alle Wurzeln β der Congruenz $\eta\beta \equiv 0$ (mod. $\mathfrak{a}$) bilden ein in $\mathfrak{a}$ aufgehendes Ideal $\mathfrak{b}$, welches von $\mathfrak{o}$ verschieden ist, weil es die Zahl 1 nicht enthält; ist $\mathfrak{b}$ ein Primideal, so ist der Satz bewiesen. Ist $\mathfrak{b}$ kein Primideal, giebt es also zwei durch $\mathfrak{b}$ nicht theilbare Zahlen η', ϱ', deren Product $\eta'\varrho' \equiv 0$ (mod. $\mathfrak{b}$) ist, so bilden alle Wurzeln γ der Congruenz $\eta'\gamma \equiv 0$ (mod. $\mathfrak{b}$), d. h. der Congruenz $\eta\eta'\gamma \equiv 0$ (mod. $\mathfrak{a}$), ein in $\mathfrak{b}$ aufgehendes Ideal $\mathfrak{c}$, und zwar ist (zufolge 2.) $N(\mathfrak{c}) < N(\mathfrak{b})$, weil ϱ' in $\mathfrak{c}$, aber nicht in $\mathfrak{b}$ enthalten ist; ausserdem ist $\mathfrak{c}$ von $\mathfrak{o}$ verschieden, weil η' nicht in $\mathfrak{b}$, und folglich die Zahl 1 nicht in $\mathfrak{c}$ enthalten ist; ist $\mathfrak{c}$ ein Primideal, so ist der Satz bewiesen. Ist aber $\mathfrak{c}$ kein Primideal, so kann man in derselben Weise fortfahren; endlich muss in der Reihe der Ideale $\mathfrak{b}, \mathfrak{c}, \mathfrak{d}\ldots$, deren Normen immer kleiner werden, aber stets > 1 bleiben, ein Primideal $\mathfrak{p}$ auftreten, welches aus allen Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. $\mathfrak{a}$) besteht, wo $\nu = \eta\eta'\eta''\ldots$ durch η theilbar ist.

4. Ist μ eine von Null verschiedene Zahl in $\mathfrak{o}$ und keine Einheit, so existirt zufolge des zuletzt bewiesenen Satzes (in welchem man $\eta = 1$ nehmen kann) jedenfalls eine Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. μ) ein Primideal $\mathfrak{p}$ bilden; Primideale, welche aus den sämmtlichen Wurzeln einer solchen Congruenz bestehen, wollen wir vorläufig *einfache* Ideale nennen. Ist nun r irgend ein ganzer rationaler, nicht negativer Exponent, so bilden alle Wurzeln ϱ der Congruenz $\varrho\nu^r \equiv 0$ (mod. μ^r) ein Ideal, welches die $r$te *Potenz* von $\mathfrak{p}$ heissen und mit $\mathfrak{p}^r$ bezeichnet werden soll. Diese Definition ist unabhängig von dem zur Definition von $\mathfrak{p}$ benutzten Zahlenpaar μ, ν; ist nämlich μ' irgend eine von Null verschiedene, durch $\mathfrak{p}$ theilbare Zahl, also $\nu\mu' = \mu\nu'$, so folgt aus $\varrho\nu^r \equiv 0$ (mod. μ^r) durch Multiplication mit μ'^r und Division durch μ^r auch $\varrho\nu'^r \equiv 0$ (mod. μ'^r), und umgekehrt. Von der grössten Wichtigkeit sind aber die folgenden Sätze über einfache Ideale $\mathfrak{p}$:

Ist $s \geqq r$, so ist $\mathfrak{p}^s$ theilbar durch $\mathfrak{p}^r$. Ist nämlich σ in $\mathfrak{p}^s$ enthalten, also $\sigma\nu^s = \tau\mu^s$, so folgt, dass

$$\left(\frac{\sigma\nu^r}{\mu^r}\right)^s = \tau^r\sigma^{s-r}$$

eine ganze Zahl ist; mithin ist (nach §. 160, 3.) der jedenfalls dem Körper Ω angehörige Quotient $\sigma\nu^r : \mu^r$ ebenfalls eine *ganze* Zahl, also in $\mathfrak{o}$ enthalten, weil $\mathfrak{o}$ *alle* ganzen Zahlen des Körpers Ω umfasst*); also ist jede Zahl σ des Ideals $\mathfrak{p}^s$ auch in $\mathfrak{p}^r$ enthalten.

Ist ϱ eine von Null verschiedene Zahl in $\mathfrak{o}$, so giebt es immer eine höchste in ϱ aufgehende Potenz von $\mathfrak{p}$. Wäre nämlich für unendlich viele Exponenten r das Product $\varrho\nu^r$ theilbar durch μ^r, so müsste, da nur eine endliche Anzahl incongruenter Zahlen (mod. ϱ) existirt, für zwei *verschiedene* solche Exponenten r, s nothwendig einmal

$$\frac{\varrho\nu^r}{\mu^r} \equiv \frac{\varrho\nu^s}{\mu^s} \pmod{\varrho}, \quad \left(\frac{\nu}{\mu}\right)^r = \left(\frac{\nu}{\mu}\right)^s + \omega$$

werden, wo ω eine ganze Zahl; hieraus würde aber (nach §. 160, 3.) folgen, dass ν durch μ theilbar wäre, was nicht der Fall ist, weil sonst $\mathfrak{p} = \mathfrak{o}$ wäre.

Sind $\mathfrak{p}^r$, $\mathfrak{p}^s$ resp. die höchsten in ϱ, σ aufgehenden Potenzen, so ist $\mathfrak{p}^{r+s}$ die höchste in $\varrho\sigma$ aufgehende Potenz von $\mathfrak{p}$. Denn da $\varrho\nu^r = \varrho'\mu^r$, $\sigma\nu^s = \sigma'\mu^s$, und keins der Producte $\nu\varrho'$, $\nu\sigma'$ durch μ theilbar ist, so folgt $\varrho\sigma\nu^{r+s} = \varrho'\sigma'\mu^{r+s}$, und $\nu\varrho'\sigma'$ kann nicht durch μ theilbar sein, weil $\mathfrak{p}$ ein Primideal ist.

Ist $e \geqq 1$ der Exponent der höchsten in μ selbst aufgehenden Potenz von $\mathfrak{p}$, also $\mu\nu^e = \varkappa\mu^e$, wo $\nu\varkappa$ *nicht* theilbar durch μ, so folgt $\nu^e = \varkappa\mu^{e-1}$, d. h. der Exponent der höchsten in ν aufgehenden Potenz von $\mathfrak{p}$ ist $= e - 1$. Das Ideal $\mathfrak{p}^e$ besteht aus den sämmtlichen Wurzeln θ der Congruenz $\varkappa\theta \equiv 0 \pmod{\mu}$. Die ganze Zahl $\lambda = \varkappa\mu : \nu = \sqrt[e]{\mu\varkappa^{e-1}}$ ist durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ theilbar; mithin ist λ^r durch $\mathfrak{p}^r$, aber nicht durch $\mathfrak{p}^{r+1}$ theilbar, woraus beiläufig folgt, dass die Ideale $\mathfrak{p}^r$ und $\mathfrak{p}^{r+1}$ wirklich *verschieden* sind. Endlich leuchtet folgender Satz ein:

Jede Potenz $\mathfrak{p}^r$ eines einfachen Ideals $\mathfrak{p}$ ist durch kein von $\mathfrak{p}$ verschiedenes Primideal theilbar. Ist nämlich π irgend eine Zahl in $\mathfrak{p}$, so muss ein in $\mathfrak{p}^r$ aufgehendes Primideal in π^r, also (zufolge 3.) in π selbst, d. h. in $\mathfrak{p}$ aufgehen und folglich mit $\mathfrak{p}$ identisch sein.

5. Die Wichtigkeit der einfachen Ideale und ihre Analogie mit den rationalen Primzahlen tritt unmittelbar hervor in dem folgenden Hauptsatz:

---

*) Sobald diese Bedingung nicht erfüllt ist, verlieren auch die obigen Sätze ihre *allgemeine* Gültigkeit; dies ist von Wichtigkeit für die Erweiterung der Definition der Ideale (vergl. §. 165, 4.).

Wenn alle in einer von Null verschiedenen Zahl μ aufgehenden Potenzen einfacher Ideale auch in einer Zahl η aufgehen, so ist η durch μ theilbar. Ist η *nicht* theilbar durch μ, so giebt es (zufolge 3.) eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. μ) ein in μ aufgehendes einfaches Ideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in μ aufgehende Potenz, so ist (nach 4.) $\mathfrak{p}^{e-1}$ die höchste in ν aufgehende Potenz, und da ν durch η theilbar ist, so kann η *nicht* durch $\mathfrak{p}^e$ theilbar sein, was zu beweisen war. Derselbe Satz lässt sich offenbar auch so aussprechen: *Jedes Hauptideal* $\mathfrak{i}(\mu)$ *ist das kleinste gemeinschaftliche Multiplum aller in* μ *aufgehenden Potenzen von einfachen Idealen.* Es folgt zunächst:

Jedes Primideal $\mathfrak{p}$ *ist ein einfaches Ideal.* Es sei μ irgend eine von Null verschiedene Zahl in $\mathfrak{p}$, so muss $\mathfrak{p}$ (zufolge 3.) in einer der Potenzen einfacher Ideale aufgehen, deren kleinstes gemeinschaftliches Multiplum $\mathfrak{i}(\mu)$ ist; mithin ist $\mathfrak{p}$ selbst (zufolge 4.) ein einfaches Ideal. — Wir sprechen daher künftig nur noch von Primidealen, nicht mehr von einfachen Idealen.

Wenn alle in einem Ideal $\mathfrak{m}$ *aufgehenden Potenzen von Primidealen auch in einer Zahl* η *aufgehen, so ist* η *theilbar durch* $\mathfrak{m}$. Ist η *nicht* theilbar durch $\mathfrak{m}$, so giebt es (nach 3.) eine durch η theilbare Zahl ν der Art, dass alle Wurzeln π der Congruenz $\nu\pi \equiv 0$ (mod. $\mathfrak{m}$) ein Primideal $\mathfrak{p}$ bilden; ist $\mathfrak{p}^e$ die höchste in $\mathfrak{m}$ aufgehende Potenz von $\mathfrak{p}$, so giebt es in $\mathfrak{m}$ eine nicht durch $\mathfrak{p}^{e+1}$ theilbare Zahl μ, und das aus allen Wurzeln ϱ der Congruenz $\nu\varrho \equiv 0$ (mod. μ) bestehende Ideal $\mathfrak{r}$ ist theilbar durch $\mathfrak{p}$, weil $\nu\varrho \equiv 0$ (mod. $\mathfrak{m}$) ist. Sind nun $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$ die sämmtlichen höchsten in μ aufgehenden Potenzen verschiedener Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'' \ldots$, so besteht $\mathfrak{r}$ zufolge des obigen Hauptsatzes aus allen gemeinschaftlichen Wurzeln ϱ der Congruenzen $\nu\varrho \equiv 0$ (mod. $\mathfrak{p}^e$), $\nu\varrho \equiv 0$ (mod. $\mathfrak{p}'^{e'}$), $\nu\varrho \equiv 0$ (mod. $\mathfrak{p}''^{e''}$) u. s. w., d. h. $\mathfrak{r}$ ist das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{q}''$ . . ., welche resp. aus den Wurzeln jeder einzelnen dieser Congruenzen bestehen; da nun die Ideale $\mathfrak{q}'$, $\mathfrak{q}''$ . . . als Theiler von $\mathfrak{p}'^{e'}$, $\mathfrak{p}''^{e''}$ . . . nicht durch $\mathfrak{p}$ theilbar sind, so muss, weil $\mathfrak{r}$ durch $\mathfrak{p}$ theilbar ist, auch $\mathfrak{q}$ (zufolge 3.) durch $\mathfrak{p}$ theilbar sein; es kann folglich $\mathfrak{p}^e$ nicht in ν aufgehen (weil sonst $\mathfrak{q} = \mathfrak{o}$, also nicht durch $\mathfrak{p}$ theilbar wäre), und da ν durch η theilbar ist, so kann $\mathfrak{p}^e$ auch *nicht* in η aufgehen, was zu beweisen war.

Dieser *Fundamentalsatz* lässt sich offenbar auch so aussprechen: *Jedes Ideal ist das kleinste gemeinschaftliche Multiplum aller in ihm aufgehenden Potenzen von Primidealen.* Er entspricht durchaus

dem Fundamentalsatze der rationalen Zahlentheorie über die Zusammensetzung der Zahlen aus Primzahlen (§. 8); denn ihm zufolge ist jedes Ideal $\mathfrak{m}$ *vollständig bestimmt*, sobald die höchsten in $\mathfrak{m}$ aufgehenden Potenzen $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$ von Primidealen gegeben sind; aus ihm ergiebt sich auch ohne Weiteres der folgende Satz: *Ein Ideal* $\mathfrak{m}$ *ist stets und nur dann durch ein Ideal* $\mathfrak{d}$ *theilbar, wenn alle in* $\mathfrak{d}$ *aufgehenden Potenzen von Primidealen auch in* $\mathfrak{m}$ *aufgehen.* Dies folgt unmittelbar aus dem Begriffe des kleinsten gemeinschaftlichen Multiplums.

Ist $\mathfrak{m}$ *das kleinste gemeinschaftliche Multiplum von* $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$, *wo* $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'' \ldots$ *von einander verschiedene Primideale bedeuten, so ist* $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{p}')^{e'} N(\mathfrak{p}'')^{e''} \ldots$ Es giebt immer (zufolge 4.) eine durch $\mathfrak{p}^{e-1}$, aber nicht durch $\mathfrak{a} = \mathfrak{p}^e$ theilbare Zahl η; das aus allen Wurzeln ϱ der Congruenz $\eta\varrho \equiv 0$ (mod. $\mathfrak{a}$) bestehende Ideal $\mathfrak{r}$ ist verschieden von $\mathfrak{o}$ (weil es die Zahl 1 nicht enthält) und ein Theiler von $\mathfrak{p}$ (zufolge 4.), folglich identisch mit $\mathfrak{p}$; da ferner der grösste gemeinschaftliche Theiler $\mathfrak{d}$ der Ideale $\mathfrak{a} = \mathfrak{p}^e$ und $\mathfrak{i}(\eta)$ zufolge des eben bewiesenen Fundamentalsatzes $= \mathfrak{p}^{e-1}$ ist, so folgt (aus 2.) $N(\mathfrak{a}) = N(\mathfrak{r}) N(\mathfrak{d})$, d. h. $N(\mathfrak{p}^e) = N(\mathfrak{p}) N(\mathfrak{p}^{e-1})$, und hieraus allgemein $N(\mathfrak{p}^e) = N(\mathfrak{p})^e$. — Nun ist (zufolge der Definition 2.) das kleinste gemeinschaftliche Multiplum $\mathfrak{m}$ der Ideale $\mathfrak{p}^e, \mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$ zugleich auch das der Ideale $\mathfrak{a} = \mathfrak{p}^e$ nnd $\mathfrak{b}$, wo $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Ideale $\mathfrak{p}'^{e'}, \mathfrak{p}''^{e''} \ldots$ bedeutet; da ferner (zufolge des Fundamentalsatzes) $\mathfrak{o}$ der grösste gemeinschaftliche Theiler von $\mathfrak{a}$ und $\mathfrak{b}$ ist, so folgt (aus 2.) $N(\mathfrak{m}) = N(\mathfrak{a}) N(\mathfrak{b})$, d. h. $N(\mathfrak{m}) = N(\mathfrak{p})^e N(\mathfrak{b})$ und hieraus ergiebt sich offenbar der zu beweisende Satz.

6. Multiplicirt man alle Zahlen eines Ideals $\mathfrak{a}$ mit allen Zahlen eines Ideals $\mathfrak{b}$, so bilden diese Producte und deren Summen ein durch $\mathfrak{a}$ und $\mathfrak{b}$ theilbares Ideal, welches das *Product aus den Factoren* $\mathfrak{a}$ *und* $\mathfrak{b}$ heissen und mit $\mathfrak{a}\mathfrak{b}$ bezeichnet werden soll. Aus dieser Erklärung leuchtet sofort ein, dass $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, ferner $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$ ist (vergl. §§. 1, 2, 147). Zugleich gilt folgender Satz:

Sind $\mathfrak{p}^a, \mathfrak{p}^b$ *resp. die höchsten in* $\mathfrak{a}, \mathfrak{b}$ *aufgehenden Potenzen des Primideals* $\mathfrak{p}$, *so ist* $\mathfrak{p}^{a+b}$ *die höchste in* $\mathfrak{a}\mathfrak{b}$ *aufgehende Potenz von* $\mathfrak{p}$; *und es ist* $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) N(\mathfrak{b})$.

Aus der Erklärung folgt nämlich unmittelbar (mit Rücksicht auf 4.), dass $\mathfrak{a}\mathfrak{b}$ durch $\mathfrak{p}^{a+b}$ theilbar ist; da ferner in $\mathfrak{a}$ eine durch $\mathfrak{p}^{a+1}$ nicht theilbare Zahl α, in $\mathfrak{b}$ eine durch $\mathfrak{p}^{b+1}$ nicht theilbare

Zahl β existirt, so giebt es in $\mathfrak{a}\mathfrak{b}$ eine durch $\mathfrak{p}^{a+b+1}$ nicht theilbare Zahl $\alpha\beta$, womit der erste Theil des Satzes bewiesen ist. Ist also $\mathfrak{a}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$ ... der von einander verschiedenen Primideale $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ..., und $\mathfrak{b}$ das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^b$, $\mathfrak{p}'^{b'}$, $\mathfrak{p}''^{b''}$..., so ist $\mathfrak{a}\mathfrak{b}$ dasjenige der Potenzen $\mathfrak{p}^{a+b}$, $\mathfrak{p}'^{a'+b'}$, $\mathfrak{p}''^{a''+b''}$..., woraus (mit Rücksicht auf 5.) auch der zweite Theil des Satzes folgt.

Da aus diesem Satze auch $\mathfrak{p}^a\mathfrak{p}^b = \mathfrak{p}^{a+b}$ folgt, so ist die oben (in 4.) gewählte Ausdrucks- und Bezeichnungsweise gerechtfertigt. Sind ferner $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ ... von einander verschiedene Primideale, so ist $\mathfrak{p}^a\mathfrak{p}'^{a'}\mathfrak{p}''^{a''}$ ... das kleinste gemeinschaftliche Multiplum der Potenzen $\mathfrak{p}^a$, $\mathfrak{p}'^{a'}$, $\mathfrak{p}''^{a''}$ ... Auch leuchtet ein, dass der Begriff der Potenz durch die Definition $\mathfrak{a}^{r+1} = \mathfrak{a}\mathfrak{a}^r$ auf jedes Ideal $\mathfrak{a}$ ausgedehnt werden kann. Ist endlich $\mathfrak{a}$ *theilbar* durch $\mathfrak{d}$, so giebt es immer ein und nur ein Ideal $\mathfrak{r}$ der Art, dass $\mathfrak{a} = \mathfrak{r}\mathfrak{d}$ wird; sind nämlich $\mathfrak{p}^a$, $\mathfrak{p}^d$ die höchsten resp. in $\mathfrak{a}$, $\mathfrak{d}$ aufgehenden Potenzen eines Primideals $\mathfrak{p}$, so ist $d \leqq a$, und $\mathfrak{r}$ ist das Product aus allen Potenzen $\mathfrak{p}^{a-d}$. Mit Rücksicht hierauf erkennt man leicht, dass die früheren Sätze (in 2.) sich jetzt einfacher aussprechen lassen.

7. Wir nennen nun $\mathfrak{a}$ und $\mathfrak{b}$ *relative Primideale*, wenn ihr grösster gemeinschaftlicher Theiler $= \mathfrak{o}$ ist; ebenso soll η *relative Primzahl zum Ideal* $\mathfrak{a}$ heissen, wenn $\mathfrak{a}$ und $\mathfrak{i}(\eta)$ relative Primideale sind. Es leuchtet dann ein, dass die Sätze der rationalen Zahlentheorie über relative Primzahlen sich leicht auf die Theorie der Ideale übertragen lassen; wir begnügen uns aber hier, folgenden wichtigen Satz zu beweisen (vergl. §. 25):

Sind $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale, und μ, ν zwei gegebene Zahlen, so giebt es immer eine und nur eine Classe von Zahlen η (mod. $\mathfrak{a}\mathfrak{b}$), welche den Bedingungen $\eta \equiv \mu$ (mod. $\mathfrak{a}$), $\eta \equiv \nu$ (mod. $\mathfrak{b}$) genügen. Durchlaufen nämlich μ, ν, η vollständige Restsysteme resp. für die drei Moduln $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, so entspricht jeder Zahl η eine und nur eine Combination μ, ν der Art, dass $\mu \equiv \eta$ (mod. $\mathfrak{a}$), $\nu \equiv \eta$ (mod. $\mathfrak{b}$) ist; entspräche ferner zwei verschiedenen Zahlen η, η' des Restsystems für den Modul $\mathfrak{a}\mathfrak{b}$ eine und dieselbe Combination μ, ν, so wäre $\eta - \eta'$ theilbar sowohl durch $\mathfrak{a}$ als durch $\mathfrak{b}$, also auch durch $\mathfrak{a}\mathfrak{b}$ (weil $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale sind), mithin wäre $\eta \equiv \eta'$ (mod. $\mathfrak{a}\mathfrak{b}$), was gegen die Voraussetzung streitet. Durchläuft daher η alle seine Werthe, deren Anzahl $= N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ ist, so entstehen ebensoviele *verschiedene* Combinationen μ, ν; und da genau ebensoviele ver-

schiedene Combinationen μ, ν wirklich existiren, so muss auch umgekehrt jede Combination μ, ν einer Zahl η entsprechen, was zu beweisen war.

Bedeutet $\psi(\mathfrak{a})$ die Anzahl der (mod. $\mathfrak{a}$) incongruenten relativen Primzahlen zu $\mathfrak{a}$, so ist $\psi(\mathfrak{a}\mathfrak{b}) = \psi(\mathfrak{a})\,\psi(\mathfrak{b})$, wenn $\mathfrak{a}$, $\mathfrak{b}$ relative Primideale bedeuten. Ist ferner $\mathfrak{p}$ ein Primideal, und $e \geqq 1$, so ist $\psi(\mathfrak{p}^e) = N(\mathfrak{p}^e) - N(\mathfrak{p}^{e-1}) = N(\mathfrak{p})^{e-1}(N(\mathfrak{p}) - 1)$; denn, wenn δ alle r durch $\mathfrak{p}$ theilbaren und nach dem Modul $\mathfrak{p}^e$ incongruenten Zahlen, wenn ferner γ ein vollständiges Restsystem (mod. $\mathfrak{p}$) durchläuft, so bilden die Zahlen $\gamma + \delta$ (zufolge 2.) ein vollständiges Restsystem (mod. $\mathfrak{p}^e$), und es ist $N(\mathfrak{p}^e) = r N(\mathfrak{p})$, also $r = N(\mathfrak{p}^{e-1})$; nun ist aber eine solche Zahl $\gamma + \delta$ stets und nur dann relative Primzahl zu $\mathfrak{p}^e$, wenn γ nicht $\equiv 0$ (mod. $\mathfrak{p}$) ist, und folglich ist die Anzahl der Zahlen $\gamma + \delta$, welche relative Primzahlen zu $\mathfrak{p}^e$ sind, gleich $r(N(\mathfrak{p}) - 1)$, was zu beweisen war.

Bedeutet $\mathfrak{p}$ ein Primideal, so giebt es (zufolge 4.) immer eine Zahl λ, welche durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ theilbar ist, mithin auch eine Zahl λ^e, welche durch $\mathfrak{p}^e$, aber nicht durch $\mathfrak{p}^{e+1}$ theilbar ist. Sind nun $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'' \ldots$ von einander verschiedene Primideale, und haben $\lambda', \lambda'' \ldots$ ähnliche Bedeutung für $\mathfrak{p}', \mathfrak{p}'' \ldots$, wie λ für $\mathfrak{p}$, so existirt immer, wenn $e, e', e'' \ldots$ gegebene Exponenten bedeuten, eine Zahl η, welche den gleichzeitigen Congruenzen

$$\eta \equiv \lambda^e \text{ (mod. } \mathfrak{p}^{e+1}), \quad \eta \equiv \lambda'^{e'} \text{ (mod. } \mathfrak{p}'^{e'+1}),$$
$$\eta \equiv \lambda''^{e''} \text{ (mod. } \mathfrak{p}''^{e''+1}) \ldots$$

genügt, weil die Moduln relative Primideale sind. Dann ist offenbar $\mathfrak{i}(\eta) = \mathfrak{m}\,\mathfrak{p}^e \mathfrak{p}'^{e'} \mathfrak{p}''^{e''} \ldots$, und das Ideal $\mathfrak{m}$ ist durch keines der Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}''$ theilbar. Hieraus folgt unmittelbar der Satz:

Sind $\mathfrak{a}$, $\mathfrak{b}$ *zwei beliebige Ideale, so giebt es immer ein solches relatives Primideal* $\mathfrak{m}$ *zu* $\mathfrak{b}$, *dass* $\mathfrak{a}\mathfrak{m}$ *ein Hauptideal wird.* Sind nämlich $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'' \ldots$ alle von einander verschiedenen in $\mathfrak{a}\mathfrak{b}$ aufgehenden Primideale, und ist $\mathfrak{a} = \mathfrak{p}^e \mathfrak{p}'^{e'} \mathfrak{p}''^{e''} \ldots$ (wo die Exponenten $e, e', e'' \ldots$ auch $= 0$ sein können), so giebt es, wie eben gezeigt ist, ein durch $\mathfrak{a}$ theilbares Hauptideal $\mathfrak{i}(\eta) = \mathfrak{a}\mathfrak{m}$ der Art, dass $\mathfrak{b}$ und $\mathfrak{m}$ relative Primideale sind.

Hieraus folgt auch, dass jedes Ideal $\mathfrak{a}$, welches kein Hauptideal ist, immer als der grösste gemeinschaftliche Theiler von *zwei* Hauptidealen angesehen werden kann; hat man nämlich nach Belieben ein durch $\mathfrak{a}$ theilbares Hauptideal $\mathfrak{i}(\eta') = \mathfrak{a}\mathfrak{b}$ gewählt, so kann man immer ein zweites $\mathfrak{i}(\eta) = \mathfrak{a}\mathfrak{m}$ so wählen, dass $\mathfrak{b}$ und $\mathfrak{m}$ re-

lative Primideale werden; die sämmtlichen Zahlen des Ideals $\mathfrak{a}$ sind dann von der Form $\eta\omega + \eta'\omega'$, wo ω, ω' alle Zahlen in $\mathfrak{o}$ durchlaufen.

§. 164.

Wir gehen nun zu einer Eintheilung der Ideale des Körpers Ω in *Classen* über, welche auf folgenden Grundlagen beruht.

1. Das System E aller Hauptideale besitzt folgende fundamentale Eigenschaften*).

I. *Jedes Product aus zwei Idealen in E ist wieder ein Ideal in E.* Denn es ist $\mathfrak{i}(\eta)\mathfrak{i}(\eta') = \mathfrak{i}(\eta\eta')$.

II. *Sind $\mathfrak{e}$ und $\mathfrak{e}\mathfrak{e}'$ Ideale in E, so ist auch $\mathfrak{e}'$ ein Ideal in E.* Ist nämlich $\mathfrak{e} = \mathfrak{i}(\eta)$, $\mathfrak{e}\mathfrak{e}' = \mathfrak{i}(\eta'')$, so ist η'' theilbar durch η, also $\eta'' = \eta\eta'$, woraus $\mathfrak{e}' = \mathfrak{i}(\eta')$ folgt.

III. *Ist $\mathfrak{a}$ ein beliebiges Ideal, so giebt es immer ein Ideal $\mathfrak{m}$ der Art, dass $\mathfrak{a}\mathfrak{m}$ ein Ideal in E wird.* Denn es sei η irgend eine von Null verschiedene Zahl in $\mathfrak{a}$, so ist das Ideal $\mathfrak{e} = \mathfrak{i}(\eta)$ theilbar durch $\mathfrak{a}$, und folglich existirt (nach §. 163, 6. oder 7.) ein Ideal $\mathfrak{m}$, welches der Bedingung $\mathfrak{a}\mathfrak{m} = \mathfrak{e}$ genügt.

Wir nennen nun zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ *äquivalent*, wenn ein Ideal $\mathfrak{m}$ der Art existirt, dass beide Producte $\mathfrak{a}\mathfrak{m}$, $\mathfrak{a}'\mathfrak{m}$ dem System E angehören**). Sind ferner $\mathfrak{a}'$, $\mathfrak{a}''$ äquivalent, giebt es also ein Ideal $\mathfrak{m}'$ der Art, dass $\mathfrak{a}'\mathfrak{m}'$, $\mathfrak{a}''\mathfrak{m}'$ Ideale in E sind, so gehören, wenn $\mathfrak{a}'\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$ gesetzt wird, auch die Producte $\mathfrak{a}\mathfrak{m}'' = (\mathfrak{a}\mathfrak{m})(\mathfrak{a}'\mathfrak{m}')$ und $\mathfrak{a}''\mathfrak{m}'' = (\mathfrak{a}'\mathfrak{m})(\mathfrak{a}''\mathfrak{m}')$ dem System E an (zufolge I.), d. h. die

*) Diese drei Eigenschaften sind aber nicht charakteristisch für das System E der Hauptideale, sondern sie kommen auch anderen Systemen zu, für welche dann nothwendig dieselben Gesetze der Classification gelten. Giebt es z. B. in Ω keine Einheit, deren Norm $= -1$ ist, und nimmt man ein Ideal $\mathfrak{i}(\eta)$ nur dann in das System E auf, wenn $N(\eta)$ *positiv* ist, so hat auch dieses System E dieselben drei Eigenschaften (vergl. *Kronecker: Ueber die Classenanzahl der aus Wurzeln der Einheit gebildeten complexen Zahlen;* Monatsber. d. Berliner Ak. 23. Juli 1863). Ebenso könnte man in E alle Ideale einer ganzen *Gruppe* von Classen aufnehmen, z. B. alle diejenigen, welche dem Hauptgeschlecht angehören.

**) Diese Definition kann offenbar auch durch die folgende ersetzt werden: zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ heissen äquivalent, wenn es zwei Ideale $\mathfrak{e}$, $\mathfrak{e}'$ in E giebt, welche der Bedingung $\mathfrak{a}\mathfrak{e}' = \mathfrak{a}'\mathfrak{e}$ genügen.

dem Ideale $\mathfrak{a}'$ äquivalenten Ideale $\mathfrak{a}$, $\mathfrak{a}''$ sind auch einander äquivalent. Hieraus allein folgt schon die Möglichkeit, alle Ideale in Classen einzutheilen: eine *Classe* ist der Inbegriff aller Ideale, welche einem bestimmten Ideal äquivalent sind.

Das System E selbst bildet eine solche Classe. Gehören nämlich $\mathfrak{e}$, $\mathfrak{e}'$, $\mathfrak{e}''$ diesem System an, so gilt (zufolge I.) dasselbe von den Producten $\mathfrak{e}\mathfrak{e}''$, $\mathfrak{e}'\mathfrak{e}''$, d. h. $\mathfrak{e}$, $\mathfrak{e}'$ sind äquivalent und gehören folglich in eine und dieselbe Classe. Sind umgekehrt $\mathfrak{e}$, $\mathfrak{e}'$ äquivalent, und gehört $\mathfrak{e}$ dem System E an, so gilt dasselbe von $\mathfrak{e}'$; denn, wenn $\mathfrak{e}$, $\mathfrak{e}\mathfrak{e}''$, $\mathfrak{e}'\mathfrak{e}''$ Ideale in E sind, so gehört (zufolge II.) auch $\mathfrak{e}''$, mithin auch $\mathfrak{e}'$ dem Systeme E an. Diese Classe E soll die *Hauptclasse* heissen.

Durchläuft nun $\mathfrak{a}$ alle Ideale einer Classe A, $\mathfrak{b}$ alle Ideale einer Classe B, so gehören alle Producte $\mathfrak{a}\mathfrak{b}$ einer und derselben Classe an, welche *aus A und B zusammengesetzt* heissen und mit AB bezeichnet werden soll; gehören nämlich $\mathfrak{a}\mathfrak{m}$, $\mathfrak{a}'\mathfrak{m}$, $\mathfrak{b}\mathfrak{n}$, $\mathfrak{b}'\mathfrak{n}$ der Hauptclasse E an, so gilt (zufolge I.) dasselbe von $(\mathfrak{a}\mathfrak{b})(\mathfrak{m}\mathfrak{n}) = (\mathfrak{a}\mathfrak{m})(\mathfrak{b}\mathfrak{n})$ und $(\mathfrak{a}'\mathfrak{b}')(\mathfrak{m}\mathfrak{n}) = (\mathfrak{a}'\mathfrak{m})(\mathfrak{b}'\mathfrak{n})$. Offenbar ist $AB = BA$, $(AB)C = A(BC)$ u. s. w. (vergl. §. 147).

Ist $\mathfrak{a}$ ein beliebiges Ideal, $\mathfrak{e}$ ein Ideal in E, so sind $\mathfrak{a}$ und $\mathfrak{a}\mathfrak{e}$ äquivalent; gehört nämlich $\mathfrak{a}\mathfrak{m}$ dem System E an, so gilt dasselbe von $(\mathfrak{a}\mathfrak{e})\mathfrak{m} = (\mathfrak{a}\mathfrak{m})\mathfrak{e}$. Hieraus folgt $AE = A$ (vergl. §. 148, 1.).

Da ferner jedes gegebene Ideal $\mathfrak{a}$ (zufolge III.) durch Multiplication mit einem Ideal $\mathfrak{m}$ in ein Ideal der Hauptclasse E verwandelt werden kann, so gehört zu jeder gegebenen Classe A auch eine *entgegengesetzte* Classe M (oder A^{-1}) der Art, dass $AM = E$ wird, und zwar nur eine einzige, weil aus $AM' = E$ auch $AM'M = EM$, d. h. $M' = M$ folgt. Allgemein ergiebt sich hieraus, dass aus $AB = AC$ stets $B = C$ folgt (vergl. §. 148, 2.).

2. Dass nun die Anzahl aller Idealclassen *endlich* ist, beruht auf einer tieferen Eigenschaft des Systems E aller Hauptideale, welche jetzt zu besprechen ist. Bilden die ganzen Zahlen $\omega_1, \omega_2 \dots \omega_n$ eine Grundreihe (oder irgend eine Basis) des Körpers Ω, und setzen wir (wie in §. 159) $\omega = \sum h_\iota \omega_\iota$, $H = N(\omega)$, so ist H eine homogene Function $n$ten Grades der Coordinaten h_ι mit *ganzen* rationalen Coefficienten; bedeutet nun s die Summe der absoluten Werthe dieser Coefficienten, so besteht folgender Satz:

Ist $\mathfrak{a}$ irgend ein Ideal, so giebt es immer ein durch $\mathfrak{a}$ theilbares Hauptideal, dessen Norm $\leqq s\,N(\mathfrak{a})$ ist. Man gebe jeder der n Coordinaten h_ι alle $(k+1)$ Werthe $0, 1, 2 \dots k$, wo $k \leqq \sqrt[n]{N(\mathfrak{a})} < k+1$;

da die Anzahl $(k+1)^n$ der so entstehenden ganzen Zahlen ω grösser als $N(\mathfrak{a})$ ist, so müssen zwei ungleiche von ihnen einander congruent (mod. $\mathfrak{a}$) sein; ihre Differenz η wird dann eine von Null verschiedene, durch $\mathfrak{a}$ theilbare Zahl, und da die absoluten Werthe ihrer Coordinaten den Werth k nicht übersteigen, so ist $N(\eta)$ absolut genommen $\leqq s k^n \leqq s N(\mathfrak{a})$; das Hauptideal $\mathfrak{i}(\eta)$ hat daher die geforderte Eigenschaft. Derselbe Satz kann offenbar auch so ausgesprochen werden: *Jedes Ideal* $\mathfrak{a}$ *kann in ein Hauptideal verwandelt werden durch Multiplication mit einem Ideal* $\mathfrak{m}$, *dessen Norm* $\leqq s$ *ist.*

Hierzu tritt folgende Ueberlegung. Durchläuft ϱ ein vollständiges Restsystem (mod. $\mathfrak{m}$), so nimmt auch $1+\varrho$ lauter incongruente Werthe an, woraus durch Addition leicht folgt, dass die Zahl $m = N(\mathfrak{m})$ durch $\mathfrak{m}$ theilbar, dass also $\mathfrak{m}$ ein Theiler des Hauptideals $\mathfrak{i}(m)$ ist. Da nun jedes Ideal nur eine endliche Anzahl von Theilern besitzt (§. 163, 2.), so giebt es auch nur eine endliche Anzahl von Idealen $\mathfrak{m}$, deren Normen einen gegebenen Werth m besitzen, mithin auch nur eine endliche Anzahl von Idealen $\mathfrak{m}$, deren Normen einen gegebenen Werth s nicht übertreffen. Zufolge des vorhergehenden Satzes giebt es daher eine *endliche* Anzahl von Idealen $\mathfrak{m}$ der Art, dass jedes beliebige Ideal $\mathfrak{a}$ durch Multiplication mit einem dieser Ideale $\mathfrak{m}$ in ein Hauptideal verwandelt werden kann; dieser wichtige Zusatz zu der Eigenschaft III. des Systems E kann offenbar auch so gefasst werden: *Die Anzahl der Idealclassen, d. h. die Anzahl der nicht äquivalenten Ideale ist endlich.*

3. Es leuchtet nun ein, dass alle Sätze über Perioden oder über Gruppen von Classen quadratischer Formen (§. 149) ohne Weiteres auf unsere Idealclassen übertragen werden können. Wir heben hier nur die einzige Folgerung hervor:

Jedes Ideal kann durch Potenzirung in ein Hauptideal verwandelt werden. Ist also $\mathfrak{a}$ ein Ideal, so giebt es immer einen positiven ganzen rationalen Exponenten m (Divisor der Classenanzahl) der Art, dass $\mathfrak{a}^m$ ein Hauptideal $\mathfrak{i}(\eta)$ wird; ist nun α irgend eine Zahl des Ideals $\mathfrak{a}$, so ist α^m theilbar durch η, mithin α theilbar durch die ganze Zahl $\sqrt[m]{\eta}$ (§. 160, 3.). Ist $\mathfrak{p}^e$ die höchste in $\mathfrak{a}$ aufgehende Potenz eines Primideals $\mathfrak{p}$, so ist me der Exponent der höchsten in η aufgehenden Potenz von $\mathfrak{p}$; hieraus folgt leicht, dass umgekehrt jede durch $\sqrt[m]{\eta}$ theilbare Zahl α in $\mathfrak{o}$ dem Ideale $\mathfrak{a}$ angehört; denn da

α^m theilbar durch η ist, so ist, wenn $\mathfrak{p}^a$ die höchste in α aufgehende Potenz von $\mathfrak{p}$ bedeutet, $ma \geqq me$, also $a \geqq e$, mithin geht $\mathfrak{p}^e$ auch in α auf (§. 163, 5.). *Das Ideal* $\mathfrak{a}$ *besteht daher aus allen durch* $\sqrt[m]{\eta}$ *theilbaren Zahlen in* $\mathfrak{o}$.

Eine unmittelbare Folgerung aus dem Vorhergehenden ist der wichtige Satz: *Je zwei ganze Zahlen* μ, ν *besitzen einen grössten gemeinschaftlichen Divisor* δ *der Art, dass die Quotienten* $\mu:\delta$, $\nu:\delta$ *relative Primzahlen werden.* Denn bildet man in irgend einem Körper Ω, welchem die beiden Zahlen μ, ν angehören, den grössten gemeinschaftlichen Theiler $\mathfrak{a}$ der beiden Hauptideale $\mathfrak{i}(\mu)$, $\mathfrak{i}(\nu)$, so wird, wenn $\mathfrak{a}^m = \mathfrak{i}(\eta)$ ist, $\sqrt[m]{\eta} = \delta$ ein solcher grösster gemeinschaftlicher Divisor von μ, ν; natürlich giebt es unendlich viele solche Zahlen δ, welche aber nicht wesentlich verschieden sind (§. 160, 6.).

Auf die weitere Entwicklung unserer Theorie der Ideale, wie z. B. auf die Untersuchung des Zusammenhangs zwischen den Idealen zweier verschiedenen Körper müssen wir hier verzichten.

§. 165.

Die Theorie der Ideale eines Körpers Ω hängt unmittelbar zusammen mit der Theorie der *zerlegbaren Formen*, welche demselben Körper entsprechen; wir beschränken uns hier darauf, diesen Zusammenhang in seinen Grundzügen anzudeuten.

1. Ist F ein Product aus n homogenen linearen Functionen $f_1, f_2 \ldots f_n$ von n Variabeln $h_1, h_2 \ldots h_n$, so wollen wir das Determinantenquadrat

$$\left(\Sigma \pm \frac{\partial f_1}{\partial h_1} \frac{\partial f_2}{\partial h_2} \cdots \frac{\partial f_n}{\partial h_n}\right)^2 = \Delta(F)$$

setzen und die *Determinante* der homogenen zerlegbaren Function F nennen*). Aus

$$\frac{\partial^2 \log F}{\partial h_r \partial h_s} = -\sum \frac{\partial \log f_t}{\partial h_r} \frac{\partial \log f_t}{\partial h_s}$$

folgt die Gleichung

$$F^2 \Sigma \pm \frac{\partial^2 \log F}{\partial h_1^2} \cdots \frac{\partial^2 \log F}{\partial h_n^2} = (-1)^n \Delta(F),$$

*) Für quadratische Formen ist diese Determinante das Vierfache von der in §. 53 definirten Determinante.

welcher man verschiedene andere Formen, z. B. auch die folgende

$$\begin{vmatrix} F & \frac{\partial F}{\partial h_1} & \cdots & \frac{\partial F}{\partial h_n} \\ \frac{\partial F}{\partial h_1} & \frac{\partial^2 F}{\partial h_1^2} & \cdots & \frac{\partial^2 F}{\partial h_1 \partial h_n} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial F}{\partial h_n} & \frac{\partial^2 F}{\partial h_n \partial h_1} & \cdots & \frac{\partial^2 F}{\partial h_n^2} \end{vmatrix} = (-1)^n F^{n-1} \Delta(F)$$

geben kann. Besitzt F lauter ganze rationale Coefficienten, so wollen wir ihren grössten gemeinschaftlichen Theiler t auch den *Theiler der Form F* nennen (vergl. §. 61); da sich nun leicht allgemein zeigen lässt, dass der Theiler eines Productes aus beliebigen Formen mit ganzen rationalen Coefficienten gleich dem Producte aus den Theilern der einzelnen Formen ist*), so folgt aus der vorstehenden Gleichung, dass $\Delta(F)$ eine ganze rationale, durch t^2 theilbare Zahl ist.

2. Aus der Definition eines Ideals $\mathfrak{a}$ (§. 163, 1.) ergiebt sich (zufolge §. 161), dass die sämmtlichen in ihm enthaltenen Zahlen α von der Form

$$\alpha = \sum x_\iota \alpha_\iota \qquad (1)$$

sind, wo die Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ particuläre Zahlen des Ideals $\mathfrak{a}$ bedeuten, während $x_1, x_2 \ldots x_n$ alle ganzen rationalen Zahlen durchlaufen dürfen. Bilden nun die Zahlen $\omega_1, \omega_2 \ldots \omega_n$ eine bestimmte Grundreihe des Körpers Ω (§. 162, 1.), so wollen wir die n Zahlen

$$\alpha_r = \sum a_\iota^{(r)} \omega_\iota, \qquad (2)$$

welche eine Basis des Ideals $\mathfrak{a}$ bilden, in ihrer Aufeinanderfolge immer so wählen, dass ihre Coordinaten $a_\iota^{(r)}$ eine *positive* Determinante

$$a = \sum \pm a_1' a_2'' \ldots a_n^{(n)} = N(\mathfrak{a}) \qquad (3)$$

besitzen; ferner ist die von der Wahl der Basis unabhängige Discriminante

$$\Delta(\alpha_1, \alpha_2 \ldots \alpha_n) = a^2 \Delta(\Omega). \qquad 4)$$

Damit die Zahlen α wirklich ein Ideal bilden, ist erforderlich und hinreichend, dass die sämmtlichen Producte $\alpha_\iota \omega_{\iota'}$ wieder Zahlen in $\mathfrak{a}$ sind; es wird daher

*) Vergl. *Gauss: D. A.* art. 42.

$$\alpha\omega_r = \Sigma X_r^{(\iota)}\alpha_\iota = \Sigma X_r^{(\iota)} a_{\iota'}^{(\iota)}\omega_{\iota'}, \qquad (5)$$

wo die n^2 Grössen $X_r^{(\iota)}$ homogene lineare Functionen der Veränderlichen $x_1, x_2 \ldots x_n$ mit ganzen rationalen Coefficienten bedeuten, und hieraus folgt

$$N(\alpha) = a X, \qquad (6)$$

wo die Determinante

$$X = \Sigma \pm X_1' X_2'' \ldots X_n^{(n)} \qquad (7)$$

eine homogene Form $n$ten Grades von $x_1, x_2 \ldots x_n$ bedeutet; ihre Coefficienten sind ganze rationale Zahlen, und man erkennt leicht, dass diese Form X irreductibel ist, weil sie durch die lineare Function α und folglich auch durch alle mit α conjugirten Functionen algebraisch theilbar ist (vergl. §. 159). Aus (4) und (6) folgt ihre Determinante

$$\Delta(X) = \Delta(\Omega). \qquad (8)$$

Ist ferner k eine gegebene ganze rationale (von Null verschiedene) Zahl, so kann man den Variabeln x_ι stets solche ganze rationale Werthe beilegen, dass X relative Primzahl zu k wird. Man kann nämlich $\mathfrak{a}$ durch Multiplication mit einem Ideal $\mathfrak{m}$, welches ein relatives Primideal zu $\mathfrak{i}(k)$ ist, in ein Hauptideal $\mathfrak{i}(\alpha) = \mathfrak{a}\mathfrak{m}$ verwandeln (§. 163, 7.); ist nun $\mathfrak{p}$ irgend ein in $\mathfrak{m}$ aufgehendes Primideal, und p die durch $\mathfrak{p}$ theilbare rationale Primzahl (§. 163, 3.), so kann k nicht durch p theilbar sein, und da $N(\mathfrak{m})$ ein Product aus Potenzen solcher Primzahlen p ist (§. 163, 5.), so ist $N(\mathfrak{m})$ relative Primzahl zu k. Nun ist α in $\mathfrak{a}$ enthalten, also von der Form (1), wo die Grössen x_ι bestimmte ganze rationale Werthe haben, und $N(\alpha) = a X$; da andererseits $\mathfrak{i}(\alpha) = \mathfrak{a}\mathfrak{m}$, also $N(\alpha) = \pm a N(\mathfrak{m})$ ist (§. 163, 6.), so ergiebt sich, dass $X = \pm N(\mathfrak{m})$ relative Primzahl zu k ist, was zu beweisen war (vergl. §. 93). Hieraus folgt von selbst, dass X eine *ursprüngliche* Form ist, d. h. dass ihre Coefficienten keinen gemeinschaftlichen Theiler haben.

Wenn in dem Körper Ω keine Einheit existirt, deren Norm $= -1$ ist, so wollen wir ein Hauptideal $\mathfrak{i}(\eta)$ nur dann in die Hauptclasse E aufnehmen, wenn $N(\eta)$ positiv ist; ebenso sollen zwei Ideale $\mathfrak{a}, \mathfrak{a}'$ nur dann äquivalent heissen und in dieselbe Classe aufgenommen werden, wenn beide durch Multiplication mit demselben Ideale $\mathfrak{m}$ in Ideale der Hauptclasse E verwandelt werden (vergl. §. 164. Anm.). Gehört nun das Ideal $\mathfrak{a}$ der Classe A an, so leuchtet ein, dass jeder positive Werth der Form X, welcher

ganzen rationalen Werthen x_ι entspricht, die Norm eines zur entgegengesetzten Classe A^{-1} gehörenden Ideals $\mathfrak{m}$ ist, und dass umgekehrt die Norm eines jeden solchen Ideals $\mathfrak{m}$ durch die Form X *dargestellt* werden kann.

Wählt man statt der Basiszahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ des Ideals andere $\beta_1, \beta_2 \ldots \beta_n$, welche aber ebenfalls der Bedingung genügen, dass die aus ihren Coordinaten gebildete Determinante *positiv* ist, so ist

$$\beta_r = \Sigma\, c_{r,\iota}\, \alpha_\iota, \quad \Sigma \pm c_{1,1} c_{2,2} \ldots c_{n,n} = +1, \tag{9}$$

und die der Basis $\alpha_1, \alpha_2 \ldots \alpha_n$ *entsprechende* Form X geht durch die Substitution

$$x_r = \Sigma\, c_{\iota,r}\, y_\iota, \tag{10}$$

deren Coefficienten $c_{\iota,r}$ ganze rationale Zahlen sind, in eine *äquivalente* Form Y über, welche der neuen Basis entspricht. Umgekehrt: ist Y eine mit X äquivalente Form, d. h. geht X durch eine ganzzahlige Substitution (10), deren Determinante $= +1$ ist, in Y über, so giebt es offenbar eine Basis des Ideals $\mathfrak{a}$, welcher diese Form Y entspricht. Allen Basen desselben Ideals $\mathfrak{a}$ entspricht daher eine bestimmte *Formenclasse*, d. h. ein System von Formen $X, Y \ldots$, der Art, dass je zwei von ihnen einander äquivalent sind, und wir wollen sagen, dass diese Formenclasse dem Ideale $\mathfrak{a}$ entspricht. Ist ferner η eine ganze Zahl von positiver Norm, so bilden die n Producte $\eta\alpha_\iota$ eine Basis des Ideals $\mathfrak{a}i(\eta)$, und hieraus folgt unmittelbar, dass allen mit $\mathfrak{a}$ äquivalenten Idealen, also einer ganzen Idealclasse, auch dieselbe Formenclasse entspricht. Auf die Frage, wie vielen Idealclassen eine und dieselbe Formenclasse entspricht, gehen wir hier nicht ein.

3. Bilden die Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$ die Basis eines Ideals $\mathfrak{a}$, ebenso die Zahlen $\beta_1, \beta_2 \ldots \beta_n$ die Basis eines Ideals $\mathfrak{b}$, so hängen die Basiszahlen $\gamma_1, \gamma_2 \ldots \gamma_n$ des Productes $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ mit denen der Ideale $\mathfrak{a}, \mathfrak{b}$ durch Gleichungen von der Form

$$\alpha_r \beta_s = \Sigma\, p_\iota^{r,s} \gamma_\iota, \quad \gamma_r = \Sigma\, q_r^{\iota,\iota'} \alpha_\iota \beta_{\iota'} \tag{11}$$

zusammen, wo die sämmtlichen $2n^3$ Grössen p und q ganze rationale Zahlen bedeuten; durch Substitution erhält man

$$\Sigma\, p_r^{\iota,\iota'} q_s^{\iota,\iota'} = 1 \quad \text{oder} \quad = 0, \tag{12}$$

je nachdem $r = s$ ist oder nicht. Bezeichnet man mit P alle aus den Zahlen p gebildeten Determinanten $n$ten Grades, mit Q die ent-

sprechenden Determinanten aus den Zahlen q, so folgt hieraus nach einem bekannten Satze

$$\Sigma\, PQ = 1; \tag{13}$$

also haben die Determinanten P keinen gemeinschaftlichen Theiler. Führt man nun drei Systeme von je n Variabeln x, y, z ein, und setzt

$$\alpha = \Sigma\, x_\iota \alpha_\iota,\quad \beta = \Sigma\, y_\iota \beta_\iota,\quad \gamma = \Sigma\, z_\iota \gamma_\iota, \tag{14}$$

so wird

$$N(\alpha) = a X,\quad N(\beta) = b Y,\quad N(\gamma) = c Z, \tag{15}$$

wo X, Y, Z die zu $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ gehörigen Formen bedeuten, und

$$a = N(\mathfrak{a}),\quad b = N(\mathfrak{b}),\quad c = N(\mathfrak{c}) = ab \tag{16}$$

ist. Zwischen diesen Formen findet nun folgender Zusammenhang Statt. Setzt man

$$\alpha\beta = \gamma, \tag{17}$$

so werden die Variabeln z bilineare Functionen von den Variabeln x und y, nämlich

$$z_r = \Sigma\, p_r^{\iota, \iota'} x_\iota y_{\iota'}, \tag{18}$$

und da gleichzeitig $N(\alpha)\, N(\beta) = N(\gamma)$, d. h.

$$XY = Z \tag{19}$$

wird, so geht die Form Z durch diese bilineare Substitution in das Product der beiden Formen X, Y über, und wir wollen sagen, die Form Z sei aus den beiden Formen X, Y *zusammengesetzt*. Zwischen diesen Formen und der bilinearen Substitution findet nun ein einfacher Zusammenhang Statt; da nämlich

$$\alpha\beta_r = \Sigma\, \frac{\partial z_\iota}{\partial y_r} \gamma_\iota,\quad \beta\alpha_r = \Sigma\, \frac{\partial z_\iota}{\partial x_r} \gamma_\iota \tag{20}$$

ist, so erhält man, wenn man r die Werthe $1, 2 \ldots n$ durchlaufen lässt, für Ω die n mit Ω conjugirten Körper setzt und die Determinanten nimmt,

$$X = \Sigma \pm \frac{\partial z_1}{\partial y_1} \cdots \frac{\partial z_n}{\partial y_n},\quad Y = \Sigma \pm \frac{\partial z_1}{\partial x_1} \cdots \frac{\partial z_n}{\partial x_n}; \tag{21}$$

die Formen X, Y sind daher durch die Substitution (18) völlig bestimmt. Bezeichnet man ferner mit

$$\alpha' = \Sigma\, x'_\iota \alpha_\iota \tag{22}$$

die zu α adjungirte Function (§. 159, (8) und (38)), so ist

$$N(\alpha) = aX = \alpha\alpha', \tag{23}$$

und die n Grössen x' sind homogene Functionen $(n-1)$ten Grades von den Variabeln x mit rationalen Coefficienten. Durch Multiplication mit β ergiebt sich

$$aX \sum y_\iota \beta_\iota = \gamma \alpha'; \tag{24}$$

mithin sind die n Grössen

$$v_\iota = X y_\iota \tag{25}$$

bilineare Functionen von den Variabeln x', z mit rationalen Coefficienten; da ferner

$$a \sum \frac{\partial v_\iota}{\partial x'_r} \beta_\iota = \gamma \alpha_r, \tag{26}$$

so ergiebt sich, wie oben,

$$Z = a^{n-2} \sum \pm \frac{\partial v_1}{\partial x'_1} \cdots \frac{\partial v_n}{\partial x'_n}. \tag{27}$$

Hieraus folgt, dass auch die Form Z durch die bilineare Substitution (18) vollständig bestimmt ist; denn bezeichnet man mit $u_\iota^{(r)}$ den Coefficienten des Elementes

$$\frac{\partial z_\iota}{\partial y_r} \text{ in } \sum \pm \frac{\partial z_1}{\partial y_1} \cdots \frac{\partial z_n}{\partial y_n},$$

so ist auch

$$v_r = \sum u_\iota^{(r)} z_\iota, \tag{28}$$

und die n^2 Grössen $u_\iota^{(r)}$, welche homogene Functionen $(n-1)$ten Grades der Variabeln x mit ganzen rationalen Coefficienten sind, lassen sich folglich als homogene *lineare* Functionen der n Grössen x' darstellen. Statt der letzteren kann man auch n solche lineare Functionen von den n^2 Grössen $u_\iota^{(r)}$ mit ganzen rationalen Coefficienten einführen, durch welche sich umgekehrt auch die n^2 Grössen $u_\iota^{(r)}$ als lineare Functionen mit ganzen rationalen Coefficienten darstellen lassen. Auf die nähere Untersuchung dieser Eigenschaften der hier auftretenden bilinearen Substitutionen können wir aber nicht mehr eingehen.

4. Die ursprünglichen Formen X, welche den sämmtlichen Idealen des Körpers Ω entsprechen und alle dieselbe Determinante $\Delta(\Omega)$ besitzen, bilden nur einen speciellen Fall der Formen H, welche jeder beliebigen Basis $\omega_1, \omega_2 \ldots \omega_n$ des Körpers Ω entsprechen (§. 159). Für die Untersuchung dieser Formen ist es zweckmässig, den Begriff eines Ideals so zu erweitern, dass darunter ein System $\mathfrak{a}$ von ganzen Zahlen α des Körpers Ω verstanden wird, welche sich durch Addition, Subtraction und Multiplication reproduciren, mit der ferneren Bedingung, dass dieses System n unabhängige Zahlen enthält, oder dass, was dasselbe sagt, jede Zahl des Körpers durch Multiplication mit einer rationalen, von Null ver-

schiedenen Zahl in eine Zahl α des Systems $\mathfrak{a}$ verwandelt werden kann. Congruenzen in Bezug auf ein solches Ideal $\mathfrak{a}$ als Modul können addirt, subtrahirt und mit beliebigen Zahlen des Ideals multiplicirt werden. Von besonderer Wichtigkeit ist aber das System *aller* Zahlen, mit welchen solche Congruenzen multiplicirt werden dürfen, d. h. aller Zahlen, welche durch Multiplication mit allen Zahlen des Ideals $\mathfrak{a}$ in Zahlen desselben Ideals $\mathfrak{a}$ verwandelt werden; man erkennt sofort, dass dies System selbst ein Ideal ist, welches die Zahl 1 enthält. Dieses Ideal kann die *Ordnung von* $\mathfrak{a}$ oder auch ein *Einheitsideal* genannt werden, weil für die in ihm enthaltenen Zahlen die von *Dirichlet**) aufgestellte Theorie der Einheiten gilt, und wir wollen uns im Folgenden auf die Darstellung dieser Dirichlet'schen Principien beschränken, indem wir auf die weitere Entwicklung der allgemeinen Theorie der Ideale verzichten.

§. 166.

Wir nehmen im Folgenden an, dass die Basiszahlen $\omega_1, \omega_2 \ldots \omega_n$ des Körpers Ω zugleich die Basiszahlen einer *Ordnung* $\mathfrak{o}$ sind, d. h. dass die Zahl 1 und alle Producte $\omega_\iota \omega_{\iota'}$ *ganze* Coordinaten haben, woraus schon folgt, dass die Basiszahlen selbst ganze Zahlen sind. Die Zahlen in $\mathfrak{o}$, d. h. alle Zahlen $\omega = \sum h_\iota \omega_\iota$, deren Coordinaten h ganze rationale Zahlen sind, haben nun folgende Eigenschaften.

1. *Ist ω eine Zahl in $\mathfrak{o}$, so ist auch die zu ihr adjungirte Zahl ω' in $\mathfrak{o}$ enthalten.*

Da nämlich ω einer Gleichung $n$ten Grades mit ganzen rationalen Coefficienten genügt, deren letzter $= N(\omega) = \omega\omega'$ ist, so erhält man durch Division mit ω eine Gleichung von der Form

$$\omega' = c + c_1\omega + c_2\omega^2 + \cdots,$$

wo $c, c_1, c_2 \ldots$ ganze rationale Zahlen bedeuten; mithin ist ω' in $\mathfrak{o}$ enthalten.

2. Den mit Ω conjugirten n Körpern entsprechen ebensoviele homogene lineare Functionen ω der Coordinaten h, und ihr Product $N(\omega)$ wird, wenn die Coordinaten ganze Zahlen sind, ebenfalls

*) Vergl. §. 141, Anm.

eine ganze rationale Zahl und folglich absolut $\geqq 1$, ausgenommen, wenn alle Coordinaten verschwinden. Die n mit Ω conjugirten Körper enthalten entweder nur reelle Zahlen, oder es treten auch Paare von zwei solchen Körpern auf, dass wenn der eine die imaginäre Zahl $x + yi$ enthält, die conjugirte Zahl $x - yi$ sich in dem andern vorfindet. Wir wollen die Anzahl dieser imaginären Paare mit $n - \nu$, also die Anzahl der reellen Körper mit $2\nu - n$ bezeichnen; dann ist ν die Gesammtanzahl aller reellen Körper und imaginären Paare. Die einem imaginären Paare entsprechenden beiden Functionen ω sind von der Form $u + vi$ und $u - vi$, wo u und v zwei homogene lineare Functionen der Coordinaten bedeuten. Diese $2(n - \nu)$ Functionen u, v und die den reellen Körpern entsprechenden $(2\nu - n)$ Functionen ω bilden ein System von n reellen Functionen, die wir gemeinschaftlich mit w bezeichnen wollen, und deren Functionaldeterminante

$$= (2i)^{\nu - n} \sqrt{\Delta(\omega_1, \omega_2 \ldots \omega_n)},$$

also von Null verschieden ist, weil die Zahlen $\omega_1, \omega_2 \ldots \omega_n$ von einander unabhängig sind. Die Variabeln h sind daher umgekehrt völlig bestimmte lineare Functionen von den Grössen w; durchlaufen nun die letzteren stetig alle reellen Werthe, welche absolut kleiner als eine gegebene Constante sind, so bleiben auch die absoluten Werthe der Grössen h kleiner als eine entsprechende Constante und folglich wird auf diese Weise nur eine endliche Anzahl von Zahlen der Ordnung $\mathfrak{o}$ erzeugt, vielleicht gar keine.

Verstehen wir, wie üblich, unter dem Modulus $M(z)$ einer complexen Grösse $z = x + yi$ die positive Quadratwurzel aus $(x^2 + y^2)$, so können wir dies Resultat auch so aussprechen: *Es giebt in $\mathfrak{o}$ nur eine endliche Anzahl von Zahlen ω der Art, dass die Moduln aller mit ω conjugirten Zahlen, also auch die absoluten Werthe der Grössen w kleiner als eine vorgeschriebene Constante ausfallen.*

3. Wir theilen nun die n Körper, also auch die n Functionen ω nach Belieben in zwei Reihen, doch so, dass jede dieser Reihen wenigstens eine Function enthält, und dass je zwei Functionen $u \pm vi$ eines imaginären Paares in eine und dieselbe Reihe fallen (also ist der Fall $n = 1$ auszunehmen, ebenso der Fall $n = 2$ bei negativer Grundzahl). Bedeutet ferner c den grössten Werth, welchen die Modulsumme $\sum M(\omega_\iota)$ in irgend einer der n Functionen ω erreicht, so gilt folgender Satz:

Ist a ein beliebig kleiner, b ein beliebig grosser positiver gegebener Werth, so giebt es in $\mathfrak{o}$ eine solche Zahl ω, dass $M(\omega)$ in der ersten Reihe $< a$, in der zweiten $> b$, und dass $N(\omega)$ absolut $< (3\,e)^n$ wird.

Ist k eine bestimmte positive ganze rationale Zahl, und legt man jeder Coordinate h einen der $(k+1)$ Werthe $0, 1, 2 \ldots k$ bei, so wird durchweg $M(\omega) \leqq ek$, und die n Werthe w liegen zwischen den Grenzen $\pm ck$. Wir betrachten nun zunächst die der *ersten* Reihe angehörigen r Functionen ω oder w; da $n > r > 0$, und $k > 0$ ist, so ist auch

$$(k+1)^{\frac{n}{r}} > k^{\frac{n}{r}} + 1,$$

und folglich kann man eine positive ganze rationale Zahl m so wählen, dass

$$(k+1)^n > m^r > k^n$$

wird; setzt man nun zur Abkürzung

$$d = \frac{2\,ck}{m} < 2\,ck^{1-\frac{n}{r}},$$

so wird das Gebiet aller zwischen den Grenzen $\pm ck$ liegenden reellen Werthe durch Einschaltung der $(m-1)$ Zahlen

$$-ck + d, \quad -ck + 2d \ldots -ck + (m-1)\,d$$

in m Intervalle von gleicher Grösse d getheilt, wobei man diese $(m-1)$ Zahlen selbst nach Belieben dem einen oder anderen der beiden benachbarten Intervalle zurechnen kann. Da nun jeder der r Werthe w aus der ersten Reihe einem und nur einem dieser m Intervalle angehört, so ist m^r die Anzahl der verschiedenen denkbaren Fälle, welche die Vertheilung der r Werthe w auf diese m Intervalle darbieten kann. Da ferner, wenn jede der n Coordinaten h alle $(k+1)$ Werthe $0, 1, 2 \ldots k$ durchläuft, $(k+1)^n$ solche Systeme von r zusammengehörigen Werthen w entstehen, so müssen, weil $(k+1)^n > m^r$ ist, mindestens zwei *verschiedene* solche Werthsysteme hinsichtlich ihrer Vertheilung auf die m Intervalle vollständig übereinstimmen, in der Art, dass je zwei Werthe w', w'', welche eine und dieselbe Function w in diesen beiden Systemen annimmt, auch einem und demselben Intervall angehören. Wird nun das System der r Werthe w' durch die Coordinaten h'_i, ferner das System der r Werthe w'' durch die Coordinaten h''_i hervorgebracht, so entspricht den Coordinaten $h_i = h'_i - h''_i$ ein System von

r Werthen $w = w' - w''$, welche absolut den Werth d nicht übersteigen. Für diese ganzen Coordinaten h_ι, welche absolut $\leqq k$ sind und nicht sämmtlich verschwinden, wird daher in der *ersten* Reihe

$$M(\omega) \leqq d\sqrt{2} < 3\,c k^{1-\frac{n}{r}}.$$

Ist ferner P das Product aus den r Werthen ω der ersten Reihe, und $N(\omega) = PQ$, so ergiebt sich $M(P) < (3c)^r k^{r-n}$, $M(Q) \leqq (ck)^{n-r}$, mithin absolut

$$N(\omega) < (3c)^n.$$

Da endlich $N(\omega)$ eine von Null verschiedene ganze rationale Zahl ist, so wird $M(PQ) = M(P)M(Q) \geqq 1$, also $M(Q) > (3c)^{-r}k^{n-r}$; ist nun ω eine der $(n-r)$ Functionen der zweiten Reihe, und $Q = \omega\theta$, so ist $M(\theta) \leqq (ck)^{n-r-1}$, und folglich wird in der *zweiten* Reihe

$$M(\omega) > (3c)^{1-n}k.$$

Offenbar kann nun, wie klein auch a, und wie gross auch b sein mag, k stets so gross gewählt werden, dass $M(\omega)$ in der ersten Reihe $< a$, in der zweiten $> b$ ausfällt, während $N(\omega)$ absolut $< (3c)^n$ wird; was zu beweisen war.

4. Aus dem soeben bewiesenen Satze ergiebt sich, indem man dieselbe Eintheilung in zwei Reihen beibehält, dass man eine nie abreissende Kette von aufeinander folgenden, von Null verschiedenen Zahlen ω in $\mathfrak{o}$ aufstellen kann, deren Normen $< (3c)^n$ sind, und welche ausserdem noch die zweite Eigenschaft besitzen, dass $M(\omega)$ in der ersten Reihe kleiner, in der zweiten grösser ausfällt, als die Moduln aller *vorhergehenden* Zahlen ω und der mit ihnen conjugirten Zahlen; denn bezeichnet man mit a den kleinsten, mit b den grössten unter allen Moduln der schon gebildeten Zahlen ω und der mit ihnen conjugirten Zahlen, so giebt es zufolge des bewiesenen Satzes immer noch eine Zahl ω der Art, dass $M(\omega)$ in der ersten Reihe $< a$, in der zweiten $> b$ ausfällt, während $N(\omega)$ absolut genommen ebenfalls $< (3c)^n$ wird; diese neue Zahl ω ist daher auch von Null und von allen vorhergehenden Zahlen ω verschieden. Wir theilen nun die Zahlen ω dieser Kette in Gruppen ein, indem wir zwei von ihnen stets und nur dann in dieselbe Gruppe aufnehmen, wenn sie dieselbe Norm m besitzen, und wenn ausserdem die Coordinaten ihrer Differenz sämmtlich durch m theilbar sind; da nun die hier auftretenden Normen m ganze rationale Zahlen

und absolut $<(3c)^n$ sind, und da die Coordinaten einer Zahl ω hinsichtlich ihrer Reste (mod. m) höchstens $(\pm m)^n$ verschiedene Fälle darbieten können, so kann in dieser Kette von Zahlen ω auch nur eine *endliche* Anzahl verschiedener Gruppen auftreten, und folglich muss bei hinreichender Fortsetzung der nie abbrechenden Kette eine Zahl β in ihr erscheinen, welche mit einer früheren Zahl α in dieselbe Gruppe fällt. Dann ist also $N(\alpha) = N(\beta) = \beta\beta' = m$, und $\alpha = \beta + m\gamma = \beta(1+\gamma\beta') = \beta\varepsilon$, wo β' (zufolge 1.) und γ, folglich auch $\varepsilon = 1 + \gamma\beta'$ Zahlen in $\mathfrak{o}$ bedeuten; zugleich ergiebt sich, da $N(\alpha) = N(\beta) = N(\beta\varepsilon)$ von Null verschieden ist, $N(\varepsilon) = 1$, und aus $M(\alpha) = M(\beta)M(\varepsilon)$ folgt, dass $M(\varepsilon)$ in der ersten Reihe >1, in der zweiten <1 ist. Versteht man unter einer *Einheit* im Folgenden stets eine Zahl in $\mathfrak{o}$, deren Norm $= +1$ ist, so haben wir daher folgendes Resultat gewonnen:

Es giebt eine Einheit von der Art, dass die Moduln der mit ihr conjugirten Zahlen in der ersten Reihe >1, in der zweiten <1 sind.

5. Multiplicirt man je zwei zusammengehörige imaginäre Functionen $\omega = u \pm vi$ mit einander, so bilden diese $(n-\nu)$ Producte (u^2+v^2) und die $(2\nu - n)$ reellen Functionen ω ein System von ν reellen, theils quadratischen, theils linearen Functionen f', $f'' \ldots f^{(\nu)}$ der Coordinaten; nennt man die *reellen* Bestandtheile ihrer Logarithmen kurz die (conjugirten) *Logarithmen von* ω, so kann man das eben erhaltene Resultat auch so aussprechen:

Theilt man die ν Functionen f nach Belieben in zwei Reihen, doch so, dass jede dieser Reihen wenigstens eine Function enthält, so existirt stets eine Einheit ε, deren Logarithmen e', $e'' \ldots e^{(\nu)}$ positiv oder negativ sind, je nachdem sie der ersten oder der zweiten Reihe entsprechen.

Da die Summe der Logarithmen einer Zahl ω gleich dem reellen Bestandtheile des Logarithmen von $N(\omega)$ ist, so ist die Summe der Logarithmen e', $e'' \ldots e^{(\nu)}$ einer Einheit ε stets $= 0$; hat man daher ν beliebige Einheiten $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_\nu$, so ist die aus den zugehörigen ν^2 Logarithmen gebildete Determinante

$$\Sigma \pm e_1' e_2'' \ldots e_\nu^{(\nu)} = 0;$$

lässt man aber einen dieser Logarithmen, z. B. den letzten $e^{(\nu)}$, welcher der Function $f^{(\nu)}$ entspricht, stets weg, so gilt folgender Fundamentalsatz:

Es giebt immer ein System S von $(\nu-1)$ unabhängigen, d. h. solchen Einheiten $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_{\nu-1}$, dass die aus ihren Logarithmen gebildete Determinante

$$L = \Sigma \pm e_1' e_2'' \ldots e_{\nu-1}^{(\nu-1)}$$

einen positiven, also von Null verschiedenen Werth besitzt.

Ist nämlich $\nu = 2$, so folgt aus dem obigen Satze, wenn man f' in die erste, f'' in die zweite Reihe aufnimmt, die Existenz einer Einheit ε, für welche der Logarithme e' positiv ausfällt (hiermit ist für den nicht ausgeschlossenen Fall $n = 2$ die Theorie der Einheiten im Wesentlichen absolvirt; vergl. §. 142). Ist aber $\nu > 2$ und $m < \nu$, und hat man schon $m-1$ Einheiten $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_{m-1}$ aufgestellt, für welche die Determinante

$$\Sigma \pm e_1' e_2'' \ldots e_{m-1}^{(m-1)}$$

einen positiven Werth $E^{(m)}$ hat, so kann man mit Hülfe desselben Satzes die Existenz einer Einheit ε_m beweisen, für welche auch die Determinante

$$\Sigma \pm e_1' e_2'' \ldots e_{m-1}^{(m-1)} e_m^{(m)}$$

positiv ausfällt; ordnet man dieselbe nach den Logarithmen e_m', $e_m'' \ldots e_m^{(m)}$ der neuen Einheit ε_m, so nimmt sie die Form

$$E' e_m' + E'' e_m'' + \cdots + E^{(m-1)} e_m^{(m-1)} + E^{(m)} e_m^{(m)}$$

an, wo $E^{(m)}$ der Annahme zufolge positiv ist, während die übrigen aus den Logarithmen von $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_{m-1}$ gebildeten Determinanten $E', E'' \ldots E^{(m-1)}$ positiv, negativ oder auch $= 0$ sein können. Nimmt man nun von den Functionen $f', f'' \ldots f^{(m)}$ alle diejenigen in die erste Reihe auf, denen positive Werthe $E', E'' \ldots E^{(m)}$ entsprechen, also jedenfalls die Function $f^{(m)}$, während die übrigen und die Functionen $f^{(m+1)} \ldots f^{(\nu)}$, also jedenfalls $f^{(\nu)}$ in die zweite Reihe fallen, so existirt zufolge des obigen Satzes eine Einheit ε_m, deren Logarithmen $e_m', e_m'' \ldots e_m^{(\nu)}$ positiv oder negativ ausfallen, je nachdem sie der ersten oder zweiten Reihe entsprechen; mithin enthält das obige Aggregat mindestens ein positives Glied $E^{(m)} e_m^{(m)}$, und die übrigen Glieder sind nicht negativ, so dass das Aggregat selbst einen positiven Werth erhält, was zu beweisen war. Auf diese Weise kann man offenbar von $m = 2$ bis $m = \nu - 1$ fortschliessen, und erhält zuletzt das in dem Satze ausgesprochene Resultat.

6. Behält man die bisherigen Bezeichnungen bei, und lässt man $m_1, m_2 \dots m_{\nu-1}$ alle ganzen rationalen Zahlen von $-\infty$ bis $+\infty$ durchlaufen, so bilden die entsprechenden Zahlen

$$\eta = \varepsilon_1^{m_1} \varepsilon_2^{m_2} \dots \varepsilon_{\nu-1}^{m_{\nu-1}}$$

eine Gruppe (S) von unendlich vielen Einheiten, welche sich durch Multiplication und Division reproduciren.

Es fragt sich nun, ob ausser diesen Einheiten η noch andere existiren. Ist ε eine beliebige Einheit, deren Logarithmen e', $e'' \dots e^{(\nu)}$ sind, so giebt es, weil die Determinante L von Null verschieden ist, stets ein und nur ein System reeller Grössen x_1, $x_2 \dots x_{\nu-1}$, welche den ν Gleichungen

$$e_1' x_1 + e_2' x_2 + \dots + e_{\nu-1}' x_{\nu-1} = e'$$
$$\dots\dots\dots\dots\dots\dots$$
$$e_1^{(\nu)} x_1 + e_2^{(\nu)} x_2 + \dots + e_{\nu-1}^{(\nu)} x_{\nu-1} = e^{(\nu)}$$

genügen, deren letzte eine Folge der übrigen ist; wir nennen diese Werthe $x_1, x_2 \dots x_{\nu-1}$ kurz die *Exponenten* der Einheit ε in Bezug auf das System S der $(\nu - 1)$ unabhängigen Einheiten ε_1, $\varepsilon_2 \dots \varepsilon_{\nu-1}$; die Exponenten eines Productes entstehen offenbar durch Addition der entsprechenden Exponenten der Factoren, und die Exponenten einer Einheit η aus der Gruppe (S) sind ganze rationale Zahlen $m_1, m_2 \dots m_{\nu-1}$. Sind die Exponenten einer Einheit ε sämmtlich < 1 und nicht negativ, so soll ε eine in Bezug auf S *reducirte* Einheit heissen. Zunächst leuchtet ein, dass es nur eine *endliche* Anzahl solcher reducirten Einheiten giebt; lässt man nämlich in den vorstehenden linearen Ausdrücken linker Hand die Grössen $x_1, x_2 \dots x_{\nu-1}$ alle reellen Werthe zwischen 0 und 1 durchlaufen, so bleiben die Werthe dieser linearen Ausdrücke absolut kleiner als eine von den Coefficienten, d. h. von dem System S abhängige endliche Constante; dasselbe gilt daher von den Logarithmen $e', e'' \dots e^{(\nu)}$ einer reducirten Einheit ε, und folglich sind auch die Moduln aller mit ε conjugirten Zahlen kleiner als eine von S abhängige Constante, woraus (mit Rücksicht auf 2.) die Richtigkeit der obigen Behauptung sich unmittelbar ergiebt.

Jede beliebige Einheit ε lässt sich stets und nur auf einzige Art als ein Product aus einer reducirten Einheit ϱ und einer Einheit η aus der Gruppe (S) darstellen. Soll nämlich $\varepsilon = \varrho\eta$, also $\varepsilon\eta^{-1} = \varrho$ eine reducirte Einheit sein, so müssen, wenn x_1, $x_2 \dots x_{\nu-1}$ die Exponenten von ε bedeuten, die Exponenten m_1,

$m_2 \ldots m_{\nu-1}$ der der Gruppe (S) angehörigen Einheit η solche ganze rationale Zahlen sein, dass die Exponenten von ϱ, also die Zahlen $x_1 - m_1$, $x_2 - m_2 \ldots x_{\nu-1} - m_{\nu-1}$ sämmtlich < 1 und nicht negativ werden; dies kann immer und nur dadurch erreicht werden, dass man für $m_1, m_2 \ldots m_{\nu-1}$ resp. die grössten in den reellen Werthen $x_1, x_2 \ldots x_{\nu-1}$ enthaltenen ganzen rationalen Zahlen wählt (vergl. §§. 43, 44); also ist η und folglich auch ϱ vollständig bestimmt.

Ist r die Anzahl aller von einander verschiedenen reducirten Einheiten ϱ (unter denen sich auch die Zahl 1 befindet), und ε irgend eine Einheit, so ist ε^r eine der Gruppe (S) angehörige Einheit; durchläuft nämlich ϱ alle reducirten Einheiten, so ist jedes der r Producte $\varepsilon\varrho$ von der Form $\sigma\eta$, wo σ eine reducirte Einheit, η eine Einheit aus der Gruppe (S) bedeutet, und σ muss ebenfalls alle r reducirten Einheiten durchlaufen, weil aus $\varepsilon\varrho = \sigma\eta$ und $\varepsilon\varrho' = \sigma\eta'$ auch die Gleichung $\varrho'\eta = \varrho\eta'$ folgen würde, welche, wie oben gezeigt ist, nur dann bestehen kann, wenn $\varrho = \varrho'$ ist; multiplicirt man nun die r Gleichungen von der Form $\varepsilon\varrho = \sigma\eta$, und dividirt durch das Product der r reducirten Einheiten ϱ oder σ, so folgt, dass ε^r ein Product aus r Einheiten der Gruppe (S), mithin selbst eine Einheit dieser Gruppe ist.

Die Exponenten von ε^r sind daher immer ganze rationale Zahlen $m_1, m_2 \ldots m_{\nu-1}$, und folglich sind die Exponenten einer jeden Einheit ε stets *rationale* Zahlen mit dem gemeinschaftlichen Nenner r. Sind nun $\delta_1, \delta_2 \ldots \delta_{\nu-1}$ beliebige Einheiten, deren Logarithmen mit d bezeichnet werden, so folgt, dass die ihnen entsprechende Determinante

$$= \Sigma \pm d_1' d_2'' \ldots d_{\nu-1}^{(\nu-1)} = \frac{mL}{r^{\nu-1}}$$

ist, wo m die aus den $(\nu-1)^2$ Exponenten der Einheiten δ_1^r, $\delta_2^r \ldots \delta_{\nu-1}^r$ gebildete Determinante, also eine *ganze* rationale Zahl bedeutet, welche von Null verschieden ist, wenn $\delta_1, \delta_2 \ldots \delta_{\nu-1}$ ebenfalls ein System von unabhängigen Einheiten bilden. Hieraus ergiebt sich die wichtige Folgerung, dass es unter allen Systemen von $(\nu-1)$ unabhängigen Einheiten ein solches geben muss, für welches die entsprechende Determinante absolut genommen einen *Minimalwerth* annimmt; denn unter allen hier auftretenden ganzen rationalen, von Null verschiedenen Zahlen m muss es eine absolut kleinste geben. Ein solches System von $(\nu-1)$ unabhängigen Einheiten soll ein *Fundamentalsystem* heissen.

7. Wir wollen nun annehmen, das obige System S der $(\nu-1)$ unabhängigen Einheiten sei ein solches Fundamentalsystem, also L der eben erwähnte Minimalwerth, so folgt zunächst, dass die Exponenten $x_1, x_2 \ldots x_{\nu-1}$ einer jeden in Bezug auf S reducirten Einheit ε sämmtlich $= 0$ sind; wäre nämlich z. B. x_1 von Null verschieden, also positiv und < 1, so wäre die den $(\nu-1)$ Einheiten $\varepsilon, \varepsilon_2 \ldots \varepsilon_{\nu-1}$ entsprechende Determinante

$$\Sigma \pm e' e''_2 \ldots e^{(\nu-1)}_{\nu-1} = L x_1$$

von Null verschieden und absolut kleiner als L, was mit unserer Annahme streitet. Da ferner die Exponenten eines Productes zweier Einheiten durch Addition der entsprechenden Exponenten der beiden Factoren entstehen, so sind die Exponenten eines jeden Productes $\varrho\varrho' = \varrho''$ aus zwei reducirten Einheiten ϱ, ϱ' sämmtlich $= 0$, d. h. ein solches Product ist wieder eine reducirte Einheit. Hieraus folgt unmittelbar, dass die sämmtlichen r reducirten Einheiten ϱ die Wurzeln der Gleichung $\varrho^r = 1$ sind; durchläuft nämlich ϱ' alle reducirten Einheiten, so gilt dasselbe von $\varrho'' = \varrho\varrho'$; multiplicirt man diese r Gleichungen, und dividirt durch das Product aller reducirten Einheiten ϱ' oder ϱ'', so folgt $\varrho^r = 1$. Da endlich schon (in 6.) gezeigt ist, dass jede Einheit ε von der Form $\varrho\eta$ ist, wo ϱ eine reducirte, und η eine Einheit aus der Gruppe (S) bedeutet, so haben wir hiermit den folgenden grossen Satz von *Dirichlet* bewiesen:

Bezeichnet ν die Gesammtanzahl der reellen und imaginären Paare unter den mit Ω conjugirten Körpern, so giebt es in jeder Ordnung $\mathfrak{o}$ immer $(\nu-1)$ Fundamentaleinheiten von solcher Beschaffenheit, dass, wenn man dieselben beliebig oft in einander multiplicirt und dividirt und dem so gebildeten allgemeinen Product gewisse besondere Einheiten ϱ in endlicher Anzahl einzeln als Factor zugesellt, alle Einheiten dieser Ordnung und zwar jede nur einmal dargestellt werden; ist r die Anzahl dieser besonderen Einheiten ϱ, so sind sie die Wurzeln der Gleichung $\varrho^r = 1$.

§. 167.

Der eben bewiesene Satz bildet neben der Theorie der Ideale (§. 163) die wichtigste Grundlage für das tiefere Studium der ganzen Zahlen des Körpers Ω, und er ist unentbehrlich für die wirkliche Bestimmung der Anzahl der Idealclassen nach Dirichlet'schen Principien. Diese geschieht dadurch, dass der Grenzwerth der über alle Ideale $\mathfrak{a}$ ausgedehnten Summe

$$\Sigma \frac{s-1}{N(\mathfrak{a})^s}$$

für unendlich kleine positive Werthe von $(s-1)$ auf doppelte Weise ermittelt wird. Einmal muss das System aller Idealnormen $N(\mathfrak{a})$ genau definirt werden, d. h. es muss von jeder positiven ganzen rationalen Zahl m festgestellt werden, wie gross die Anzahl $\tau(m)$ der verschiedenen Ideale $\mathfrak{a}$ ist, deren Norm $= m$; die Beantwortung dieser Frage fällt der Theorie der Ideale zu. Die Summe nimmt dann die Form

$$(s-1)\ \Sigma \frac{\tau(m)}{m^s}$$

an, wo m alle positiven ganzen rationalen Zahlen durchlaufen muss*).

Das andere Mal theilt man die obige Summe in Partialsummen ein, deren jede alle die Glieder enthält, welche den sämmtlichen Idealen $\mathfrak{a}$ einer und derselben Classe entsprechen, und es sind bei

*) Hierbei zeigt sich, dass $\tau(mm') = \tau(m)\,\tau(m')$ ist, wenn m, m' relative Primzahlen sind; mithin ist $\tau(m)$ vollständig bekannt, wenn für jede rationale Primzahl p die Zerlegung von $\mathfrak{i}(p)$ in Primideale bekannt ist; die Primzahlen p zerfallen hiernach in eine endliche Anzahl verschiedener Arten, in der Weise, dass für alle Primzahlen p gleicher Art die Bestimmung von $\tau(p^e)$ nach derselben Regel geschieht. Die obige Summe lässt sich daher gewissen Umformungen unterwerfen, welche für *alle* Körper gültig sind; am einfachsten gestalten sich dieselben für Galois'sche Körper.

der weiteren Untersuchung hauptsächlich folgende Momente zu berücksichtigen.

Nimmt man, falls in Ω keine Einheit von der Norm -1 existirt, ein Ideal $\mathfrak{i}(\omega)$ nur dann in die Hauptclasse E auf, wenn $H = N(\omega)$ *positiv* ist, so braucht man nur alle ganzen Zahlen ω von positiver Norm zu betrachten, und es wird, wenn α eine bestimmte solche Zahl bedeutet, $\mathfrak{i}(\omega)$ stets und nur dann mit $\mathfrak{i}(\alpha)$ identisch sein, wenn $\omega = \varepsilon\alpha$, und ε eine Einheit von positiver Norm ist. Abgesehen von dem Falle eines quadratischen imaginären Körpers wird daher jedes Ideal der Hauptclasse unendlich oft auftreten, und es kommt darauf an, ω solchen Bedingungen zu unterwerfen, dass jedes Ideal $\mathfrak{i}(\omega)$ nur einmal oder wenigstens nicht unendlich oft erscheint (vergl. §. 87). Behalten wir die Bezeichnungen des vorhergehenden Paragraphen bei, indem wir annehmen, dass die Ordnung $\mathfrak{o}$ alle ganzen Zahlen des Körpers umfasst, so kann dies in folgender Weise erreicht werden.

Dividirt man jede der ν Functionen $f', f'' \ldots f^{(\nu)}$, je nachdem sie linear oder quadratisch ist, durch $\sqrt[n]{H}$ oder durch $\sqrt[n]{H^2}$, und bezeichnet man mit $l', l'' \ldots l^{(\nu)}$ die reellen Bestandtheile der Logarithmen dieser ν Quotienten, so ist $l' + l'' + \cdots + l^{(\nu)} = 0$, und es giebt stets ein und nur ein System von reellen Grössen $x_1, x_2 \ldots x_{\nu-1}$, welche den Gleichungen

$$e'_1 x_1 + e'_2 x_2 + \cdots + e'_{\nu-1} x_{\nu-1} = l'$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$e^{(\nu)}_1 x_1 + e^{(\nu)}_2 x_2 + \cdots + e^{(\nu)}_{\nu-1} x_{\nu-1} = l^{(\nu)}$$

genügen; nennen wir sie kurz die *Exponenten von* ω (vergl. §. 166,6.), so leuchtet ein, dass die Exponenten eines Productes durch Addition der entsprechenden Exponenten der Factoren entstehen. Nennt man ferner ω eine *reducirte* Zahl, wenn ihre Exponenten sämmtlich < 1 und nicht negativ sind, und lässt man ε zunächst nur alle Einheiten η durchlaufen, welche der Gruppe (S) angehören, während α eine gegebene ganze Zahl bedeutet, so ergiebt sich, dass unter allen Producten $\omega = \eta\alpha$ eine und nur eine reducirte ganze Zahl, und folglich unter allen Producten $\omega = \varepsilon\alpha$ genau r reducirte ganze Zahlen ω existiren, wenn r wieder die Anzahl der in Bezug auf S reducirten Einheiten bedeutet. Mithin ist die auf die Hauptclasse E bezügliche Partialsumme gleich

$$\frac{s-1}{r} \sum \frac{1}{N(\omega)^s} = \frac{s-1}{r} \sum \frac{1}{H^s},$$

wo ω alle reducirten ganzen Zahlen durchlaufen muss, d. h. alle ganzen Zahlen $\omega = \Sigma h_\iota \omega_\iota$ von positiver Norm H, deren Exponenten den Bedingungen

$$0 \leqq x_1 < 1,\ \ 0 \leqq x_2 < 1 \ldots 0 \leqq x_{\nu-1} < 1$$

genügen.

Zur Bestimmung des Grenzwerthes g dieser Partialsumme für unendlich kleine positive Werthe von $(s-1)$ dienen nun die von *Dirichlet* aufgestellten Principien. Bedeutet t eine über alle Grenzen wachsende positive Grösse, T die Anzahl der hier auftretenden Normen H, welche nicht grösser als t sind, und nähert sich der Quotient $T:t$ einem endlichen Grenzwerth k, so ist (§. 118)

$$g = \frac{k}{r}.$$

Um ferner den Grenzwerth k des Quotienten $T:t$ zu ermitteln, muss der von *Dirichlet* benutzte geometrische Satz (§. 120) zu dem folgenden Princip erhoben werden, welches seinen unmittelbaren Grund in dem Begriff eines vielfachen bestimmten Integrals findet: Durchlaufen die n *stetigen*, reellen Variabeln h_ι ein endliches Gebiet G von n Dimensionen, und bedeutet T', wenn δ eine beliebig kleine positive Grösse ist, die Anzahl derjenigen dem Gebiete G angehörigen Werthsysteme der Variabeln h_ι, für welche die n Quotienten $h_\iota : \delta$ *ganze rationale* Zahlen werden, so wird für unendlich kleine Werthe von δ

$$\lim (T'\delta^n) = \int dh_1\, dh_2 \ldots dh_n,$$

wo das $n$fache Integral über das Gebiet G auszudehnen ist. Definirt man nun das Gebiet G durch die obigen Bedingungen für die Exponenten $x_1, x_2 \ldots x_{\nu-1}$ von $\omega = \Sigma h_\iota \omega_\iota$ und durch die Bedingung

$$0 < H \leqq 1,$$

und bedenkt, dass die Exponenten von ω nur von den *Verhältnissen* der Variabeln h_ι abhängen, während H eine homogene Function $n$ten Grades ist, so leuchtet unmittelbar ein, dass T' durchaus identisch mit T ist, sobald

$$\delta = \frac{1}{\sqrt[n]{t}}$$

genommen wird; denn wenn die ganzen rationalen Zahlen h_ι durch $h_\iota \sqrt[n]{t} = h_\iota : \delta$ ersetzt werden, so geht die durch T reducirte ganze

Zahlen ω erfüllte Bedingung $0 < H \leqq t$ in $0 < H \leqq 1$ über, während die Bedingungen für die Exponenten ungeändert bleiben. Da zugleich $T'\delta^n = T:t$ ist, so ergiebt sich also, dass der Grenzwerth der auf die Hauptclasse E bezüglichen Partialsumme

$$g = \frac{1}{r}\int dh_1 dh_2 \ldots dh_n$$

ist.

Um den Werth dieses Integrals zu erhalten, führe man als neue unabhängige Variabele $H, x_1, x_2 \ldots x_{\nu-1}$ und die zwischen den Grenzen 0 und 2π liegenden Winkel $\varphi_1, \varphi_2 \ldots \varphi_{n-\nu}$ ein, welche den $(n-\nu)$ mit ω conjugirten imaginären Paaren $u \pm vi$ in der Weise entsprechen, dass

$$u + vi = \sqrt{f}.e^{\varphi i}, \quad f = u^2 + v^2$$

wird. Jedem System der ursprünglichen Variabeln h_ι entspricht ein und nur ein System der neuen Variabeln; umgekehrt aber entsprechen jedem System der neuen Variabeln, wenn H positiv genommen wird, $2^{2\nu-n-1}$ verschiedene Systeme der alten Variabeln h_ι; denn durch die Werthe von $H, x_1, x_2 \ldots x_{\nu-1}$ werden nur die absoluten Werthe der $(2\nu-n)$ reellen mit ω conjugirten Functionen bestimmt, und da ihr Product positiv sein muss, so kann man ihnen, mit Ausnahme einer, sowohl das positive wie das negative Vorzeichen geben; nur in dem Falle $n = 2\nu$, wenn gar kein reeller Körper mit Ω conjugirt ist, muss diese Anzahl $2^{2\nu-n-1}$ wieder durch 1 ersetzt werden. Geht man ferner von den ursprünglichen Variabeln h_ι successive zu den mit ω conjugirten oder den n Functionen w, von diesen zu $f', f'' \ldots f^{(\nu)}, \varphi_1, \varphi_2 \ldots \varphi_{n-\nu}$, von diesen zu den neuen Variabeln über, so findet man leicht, dass die entsprechende Functional-Determinante gleich

$$\frac{L}{i^{\nu-n}\sqrt{\Delta(\Omega)}} = \frac{\Sigma \pm e'_1 e''_2 \ldots e^{(\nu-1)}_{\nu-1}}{i^{\nu-n}\sqrt{\Delta(\Omega)}}$$

ist; mithin ist der auf die Hauptclasse E bezügliche Grenzwerth g gleich

$$\frac{2^{\nu-1}\pi^{n-\nu}L}{r i^{\nu-n}\sqrt{\Delta(\Omega)}},$$

oder doppelt so gross, falls $n = 2\nu$ ist (wenn zugleich $n = 2$ ist, so ist $L = 1$ zu setzen, und r bedeutet die Anzahl aller Einheiten).

An dieses Resultat knüpfen wir zunächst folgende Bemerkung. Nimmt man in die erste Partialsumme nicht alle Ideale der Haupt-

classe E, sondern nur diejenigen Ideale $\mathfrak{e}$ auf, welche zugleich durch ein bestimmtes Ideal $\mathfrak{m}$ theilbar sind, so treten an die Stelle der Basiszahlen $\omega_1, \omega_2 \ldots \omega_n$ von $\mathfrak{o}$ die Basiszahlen $\mu_1, \mu_2 \ldots \mu_n$ dieses Ideals $\mathfrak{m}$, während alles Uebrige unverändert bleibt; mithin ist $\Delta(\Omega)$ durch

$$\Delta(\mu_1, \mu_2 \ldots \mu_n) = N(\mathfrak{m})^2 \Delta(\Omega)$$

zu ersetzen, und der Grenzwerth dieser auf alle Ideale $\mathfrak{e}$ bezüglichen Summe ist $= g : N(\mathfrak{m})$.

Durchläuft nun $\mathfrak{a}$ alle Ideale einer beliebigen Classe A, so giebt es ein Ideal $\mathfrak{m}$ der Art, dass alle Producte $\mathfrak{am}$ Ideale der Hauptclasse E werden, und da umgekehrt, wenn $\mathfrak{e}$ ein durch $\mathfrak{m}$ theilbares Ideal $\mathfrak{am}$ der Hauptclasse E ist, $\mathfrak{a}$ gewiss der Classe A angehört, so ist

$$\Sigma \frac{s-1}{N(\mathfrak{a})^s} = N(\mathfrak{m})^s \, \Sigma \frac{s-1}{N(\mathfrak{e})^s},$$

und folglich

$$\lim \Sigma \frac{s-1}{N(\mathfrak{a})^s} = g,$$

d. h. jede auf eine bestimmte Idealclasse bezügliche Partialsumme nähert sich demselben Grenzwerthe g. Bezeichnet man daher mit $h(\Omega)$ die *Anzahl* aller dieser Idealclassen, so ist der Grenzwerth der Totalsumme gleich $gh(\Omega)$, und folglich ist

$$h(\Omega) = \frac{r i^{\nu-n} \sqrt{\Delta(\Omega)}}{2^{\nu-1} \pi^{n-\nu} L} \lim \Sigma \frac{(s-1)\tau(m)}{m^s}$$

oder halb so gross, wenn $n = 2\nu$ ist. Die Bestimmung der Classenanzahl ist hiermit auf die von der Theorie der Ideale zu leistende Bestimmung der Function $\tau(m)$ zurückgeführt*).

*) Für die aus der Kreistheilung entspringenden Körper führt dieselbe, wie *Kummer* gezeigt hat, zu den Reihen, welche in dem Dirichlet'schen Beweise des Satzes über die arithmetische Progression (Supplement VI) auftreten; vergl. die Anm. zu §. 163, 3.

§. 168.

Wir wollen nun zum Schlusse die vorhergehenden allgemeinen Untersuchungen auf die quadratischen Körper anwenden, um von dem gewonnenen Standpunct aus den Hauptgegenstand dieses Werkes noch einmal zu überblicken.

Ist die ganze rationale Zahl D keine Quadratzahl und auch durch kein Quadrat (ausser 1) theilbar, so bilden die Zahlen $t + u\sqrt{D}$, wenn t, u alle rationalen Zahlen durchlaufen, einen quadratischen Körper, welcher durch die beiden Substitutionen $\varphi(t + u\sqrt{D}) = t \pm u\sqrt{D}$ in sich selbst übergeht. Setzt man $\theta = \frac{1}{2}(1 + \sqrt{D})$ oder $= \sqrt{D}$, je nachdem $D \equiv 1$ (mod. 4) ist oder nicht, so bilden die Zahlen 1, θ eine Grundreihe des Körpers, und seine Grundzahl Δ ist entsprechend $= D$ oder $= 4D$. Die quadratische Gleichung, welcher θ genügt, sei

$$f(\theta) = \theta^2 - b\theta + c = 0,$$

so ist $x + y\theta$ mit $x + y(b - \theta)$ conjugirt, und

$$\Delta = (2\theta - b)^2 = b^2 - 4c.$$

Ist nun $\mathfrak{p}$ irgend ein Primideal des Körpers, und p die durch $\mathfrak{p}$ theilbare positive rationale Primzahl, so ist $N(\mathfrak{p}) = p^2$ oder $= p$, je nachdem $\mathfrak{i}(p) = \mathfrak{p}$ oder ein Product aus zwei Primidealen $\mathfrak{p}$, $\mathfrak{p}'$ ist. Im letzteren Falle bilden die Zahlen 0, 1, 2 ... $(p - 1)$, weil sie incongruent sind, ein vollständiges Restsystem (mod. $\mathfrak{p}$), d. h. jede ganze Zahl des Körpers ist einer rationalen ganzen Zahl congruent; mithin giebt es auch eine rationale ganze Zahl t, welcher θ congruent ist, und folglich ist $f(t) = t^2 - bt + c$ eine ganze rationale durch $\mathfrak{p}$, also auch durch p theilbare Zahl, d. h.

$$t^2 - bt + c \equiv 0 \text{ (mod. } p),$$

oder in der Sprache der Theorie der höheren Congruenzen: die quadratische Function $f(x) = x^2 - bx + c$ ist nach dem Modul p congruent einem Producte aus zwei Functionen ersten Grades $(x - t)$ und $(x - b + t)$ mit rationalen Coefficienten. Umgekehrt: hat die Congruenz $f(x) \equiv 0$ (mod. p) eine rationale Wurzel $x \equiv t$, so ist

$$f(t) = (t - \theta)(t - b + \theta) \equiv 0 \text{ (mod. } p);$$

wäre nun $\mathfrak{i}(p)$ ein Primideal, so müsste wenigstens einer der Factoren $(t-\theta)$, $(t-b+\theta)$ durch p theilbar sein, was aber nicht der Fall ist, weil die Zahlen $1, \theta$ eine *Grundreihe* des Körpers bilden; mithin ist $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$ ein Product aus zwei Primidealen $\mathfrak{p}$ und $\mathfrak{p}'$, deren Normen $= p$ sind; ist nun $t-\theta$ durch $\mathfrak{p}$ theilbar, also $\mathfrak{i}(t-\theta) = \mathfrak{p}\mathfrak{q}$, so ist $\mathfrak{q}$ nicht theilbar durch $\mathfrak{p}'$, weil sonst $(t-\theta)$ durch p theilbar wäre, und da $\mathfrak{i}(t-\theta)\mathfrak{i}(t-b+\theta) = \mathfrak{p}\mathfrak{q}\mathfrak{i}(t-b+\theta)$ durch $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$ theilbar ist, so muss $(t-b+\theta)$ durch $\mathfrak{p}'$ theilbar sein; man kann daher

$$\theta \equiv t \ (\text{mod. } \mathfrak{p}), \quad \theta \equiv b-t \ (\text{mod. } \mathfrak{p}')$$

setzen, und $\mathfrak{p}$, $\mathfrak{p}'$ *conjugirte* Primideale nennen, weil aus $x+y\theta \equiv 0$ (mod. $\mathfrak{p}$) stets $x+y(b-\theta) \equiv 0$ (mod. $\mathfrak{p}'$) folgt.

Es fragt sich nun, ob diese beiden Primideale $\mathfrak{p}$, $\mathfrak{p}'$ identisch sein können. Dann muss $\theta \equiv t \equiv b-t$ (mod. $\mathfrak{p}$), also $2t-b$ durch $\mathfrak{p}$ und folglich auch durch p theilbar sein, und da $4f(t) = (2t-b)^2 - \varDelta \equiv 0$ (mod. p) ist, so muss

$$\varDelta \equiv 0 \ (\text{mod. } p)$$

sein. Umgekehrt: ist p eine in der Grundzahl $\varDelta = b^2 - 4c$ aufgehende rationale Primzahl, so giebt es immer eine ganze rationale t, welche den beiden Congruenzen

$$f(t) \equiv 0, \quad 2t \equiv b \ (\text{mod. } p)$$

genügt; ist nämlich p ungerade, so ist t durch die zweite Congruenz bestimmt, und aus $4f(t) = (2t-b)^2 - \varDelta$ folgt $f(t) \equiv 0$; ist aber $p = 2$, also b gerade, so ist t durch die erste Congruenz $f(t) \equiv t^2 + c \equiv 0$ (mod. 2) bestimmt, nämlich $t \equiv c$ (mod. 2), und die zweite Congruenz ist ebenfalls erfüllt. Aus der Existenz einer rationalen Wurzel t der Congruenz $f(t) \equiv 0$ folgt aber, wie oben gezeigt ist, $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$, wo $\mathfrak{p}$ und $\mathfrak{p}'$ zwei Primideale bedeuten, für welche $\theta \equiv t$ (mod. $\mathfrak{p}$), $\theta \equiv b-t$ (mod. $\mathfrak{p}'$) ist; da nun ausserdem $t \equiv b-t$ (mod. p) ist, so folgt, dass $(\theta - t)$ sowohl durch $\mathfrak{p}$ als auch durch $\mathfrak{p}'$ theilbar ist; wären nun $\mathfrak{p}$ und $\mathfrak{p}'$ verschieden, also relative Primideale, so müsste $(\theta - t)$ auch durch $\mathfrak{p}\mathfrak{p}'$, d. h. durch p theilbar sein; da dies nicht der Fall ist, so sind $\mathfrak{p}$ und $\mathfrak{p}'$ identisch, also ist $\mathfrak{i}(p) = \mathfrak{p}^2$. Wir sind mithin zu folgendem Resultat gelangt:

Geht die rationale Primzahl p in der Grundzahl $\varDelta$ auf, so ist $\mathfrak{i}(\mathfrak{p}) = \mathfrak{p}^2$ das Quadrat eines Primideals $\mathfrak{p}$; ist p eine in $\varDelta$ nicht aufgehende Primzahl, so ist $\mathfrak{i}(p) = \mathfrak{p}\mathfrak{p}'$ ein Product aus zwei

verschiedenen Primidealen $\mathfrak{p}, \mathfrak{p}'$, *oder* $\mathfrak{i}(p)$ *ein Primideal, je nachdem die Congruenz* $f(t) \equiv 0$ *(mod. p) eine rationale Wurzel t besitzt oder nicht.*

Die Zahl $p = 2$ bietet den ersten Fall dar, wenn $\Delta \equiv 0$ (mod. 4), also $D \equiv 2, 3$ (mod. 4) ist; ist dagegen $\Delta = D \equiv 1$ (mod. 4), so tritt der zweite oder dritte Fall ein, je nachdem c gerade oder ungerade, d. h. je nachdem $D \equiv 1$ oder $\equiv 5$ (mod. 8) ist. Hieraus erklärt sich das eigenthümliche Verhalten der Zahl 2 in der Theorie der quadratischen Reste (§. 36).

Ist p eine ungerade, in Δ nicht aufgehende rationale Primzahl, so folgt aus $4f(t) = (2t-b)^2 - \Delta$, dass der zweite oder dritte Fall eintritt, je nachdem

$$\left(\frac{\Delta}{p}\right) = \left(\frac{D}{p}\right) = +1 \quad \text{oder} = -1$$

ist. Um alle Fälle am bequemsten zusammenzufassen, führen wir für jede positive ganze rationale Zahl m eine Charakteristik (Δ, m) der Art ein, dass

$$(\Delta, mm') = (\Delta, m)\,(\Delta, m')$$

und, wenn p eine rationale Primzahl bedeutet,

$$(\Delta, p) = 0, \quad = +1, \quad = -1$$

ist, je nachdem $\mathfrak{i}(p)$ Quadrat eines Primideals, oder ein Product aus zwei verschiedenen Primidealen, oder selbst ein Primideal ist. Bedeutet nun $\tau(m)$ die Anzahl aller verschiedenen Ideale $\mathfrak{a}$, deren Normen $= m$ sind, so ist

$$\tau(p^r) = (\Delta, 1) + (\Delta, p) + (\Delta, p^2) + \cdots + (\Delta, p^r),$$

und allgemein

$$\tau(m) = \Sigma\,(\Delta, n),$$

wo n alle Divisoren von m durchläuft. Hieraus folgt (vergl. §§. 89, 91, 124)

$$\Sigma\,\frac{\tau(m)}{m^s} = \Sigma\,\frac{1}{m^s}\,\Sigma\,\frac{(\Delta, m)}{m^s},$$

also, wenn $(s-1)$ positiv unendlich klein wird,

$$\lim \Sigma\,\frac{s-1}{N(\mathfrak{a})^s} = \lim\,\Sigma\,\frac{(\Delta, m)}{m^s},$$

wo m nur alle diejenigen positiven ganzen rationalen Zahlen zu durchlaufen braucht, welche relative Primzahlen zu Δ sind, oder auch

$$\lim \Sigma \frac{s-1}{N(\mathfrak{a})^s} = \frac{1}{1-\frac{(\Delta, 2)}{2}} \cdot \lim \Sigma \left(\frac{D}{n}\right) \frac{1}{n^s},$$

wo n alle relativen Primzahlen zu $2D$ durchläuft. Substituirt man dies in den allgemeinen Ausdruck des vorigen Paragraphen für die Anzahl der Idealclassen, so findet man, dass dieselbe vollständig übereinstimmt mit der Classenanzahl der (positiven) ursprünglichen Formen der Determinante D, und zwar der zweiten Art, wenn $D \equiv 1 \pmod{4}$ ist; der Grund für diese Uebereinstimmung liegt, wie man leicht erkennt, darin, dass jede Formenclasse nur einer einzigen Idealclasse entspricht (vergl. §. 165, 2.).

§. 169.

Sind α, β zwei von einander unabhängige ganze Zahlen eines quadratischen Körpers Ω, und durchlaufen die Variabeln x, y alle ganzen rationalen Zahlen, so bilden die Zahlen

$$\mu = x\alpha + y\beta \tag{1}$$

einen aus lauter ganzen Zahlen bestehenden Modul $\mathfrak{m}$ (§. 161); umgekehrt, wenn ein Modul $\mathfrak{m}$ aus ganzen Zahlen μ des Körpers Ω besteht und zwei von einander unabhängige Zahlen enthält, so sind alle Zahlen μ von der Form (1), wo α, β zwei particuläre Zahlen des Moduls bedeuten; bilden die Zahlen ω_1, ω_2 eine bestimmte Grundreihe des Körpers Ω, so kann man die Basiszahlen

$$\alpha = p_1\omega_1 + p_2\omega_2, \quad \beta = q_1\omega_1 + q_2\omega_2$$

immer so wählen, dass $(p_1q_2 - q_1p_2)$ positiv ausfällt, und dann mag α die erste, β die zweite Basiszahl des Moduls $\mathfrak{m}$ heissen. Nun wird

$$N(\mu) = m(ax^2 + bxy + cy^2), \tag{2}$$

wo m den Theiler der quadratischen Form $N(\mu)$, also eine positive ganze rationale Zahl bedeutet, während a, b, c ganze rationale Zahlen ohne gemeinschaftlichen Theiler sind. Setzt man

$$b^2 - 4ac = d, \tag{3}$$

und bezeichnet mit α_1, β_1 die resp. mit α, β conjugirten Zahlen, so ist

$$\alpha\alpha_1 = ma, \quad \alpha\beta_1 + \beta\alpha_1 = mb, \quad \beta\beta_1 = mc,$$

folglich die Discriminante

$$\Delta(\alpha, \beta) = dm^2. \qquad (4)$$

Wählt man statt α, β irgend eine andere Basis desselben Moduls $\mathfrak{m}$, so leuchtet ein, dass die Zahlen m und d unverändert bleiben, und dass die entsprechenden ursprünglichen Formen $ax^2 + bxy + cy^2$ eine Formenclasse bilden; die Zahlen m und d können füglich die *Norm* und *Determinante des Moduls* $\mathfrak{m}$ genannt werden. Ersetzt man die Variabeln x und y resp. durch β und $-\alpha$, so ergiebt sich

$$a\beta^2 - b\alpha\beta + c\alpha^2 = 0, \quad b\beta - 2c\alpha = \beta\sqrt{d}. \qquad (5)$$

Ist ausserdem

$$g = h\alpha + k\beta$$

die kleinste positive ganze rationale Zahl des Moduls $\mathfrak{m}$, so sind h, k relative Primzahlen, und wenn man

$$ah^2 + bhk + ck^2 = e$$

setzt, so ergiebt sich $N(g) = g^2 = me$; mithin ist e positiv und geht in g^2 auf. Da α, β ganze Zahlen sind, so findet man ferner leicht, dass dg^2 durch e^2 theilbar sein muss; bedeutet daher f^2 das grösste in d und e aufgehende Quadrat, so muss fg durch e theilbar sein. Soll ferner $\mathfrak{m}$ ein Ideal im weiteren Sinne des Wortes sein (§. 165, 4.), sollen also α^2, $\alpha\beta$, β^2 ebenfalls in $\mathfrak{m}$ enthalten sein, so muss g durch e theilbar sein; doch werden wir im Folgenden von dieser Voraussetzung absehen.

Suchen wir nun die *Ordnung* $\mathfrak{n}$ des Moduls $\mathfrak{m}$, d. h. das System aller Zahlen ν von der Art, dass jedes Product $\mu\nu$ in $\mathfrak{m}$ enthalten ist (§. 165, 4.), so ist erforderlich und hinreichend, dass

$$\alpha\nu = x\alpha + y\beta, \quad \beta\nu = x'\alpha + y'\beta$$

wird, wo x, y, x', y' ganze rationale Zahlen bedeuten; hieraus folgt durch Elimination von ν

$$y\beta^2 - (y' - x)\alpha\beta - x'\alpha^2 = 0,$$

und hieraus durch Vergleichung mit (5)

$$y = az, \quad y' - x = bz, \quad -x' = cz,$$

wo z eine ganze rationale Zahl sein muss, weil a, b, c keinen gemeinschaftlichen Theiler haben. Mithin wird

$$\nu = x + \frac{a\beta}{\alpha} z,$$

wo x und z willkürliche ganze rationale Zahlen bedeuten. Da aus (5)

$$N(\nu) = x^2 + bxz + acz^2$$

folgt, so sind die Norm und Determinante von $\mathfrak{n}$ resp. $= 1$ und d.

Bezeichnet man ganz allgemein die Anzahl der in einem Modul $\mathfrak{b}$ enthaltenen Zahlen, welche in Bezug auf einen Modul $\mathfrak{a}$ incongruent sind, mit $(\mathfrak{b}, \mathfrak{a})$, so ergiebt sich aus

$$g = h\alpha + k\beta$$

$$g\frac{\alpha\beta}{\alpha} = -ck\alpha + (ah + bk)\beta$$

nach leicht zu beweisenden allgemeinen Sätzen*)

$$(\mathfrak{n}, \mathfrak{m}) = \frac{g^2}{u}, \quad (\mathfrak{m}, \mathfrak{n}) = \frac{e}{u}, \quad (\mathfrak{n}, \mathfrak{m}) = m(\mathfrak{m}, \mathfrak{n}),$$

wo u den grössten gemeinschaftlichen Divisor von g und e bedeutet. Ist $\mathfrak{m}$ ein Ideal, also ein Vielfaches von $\mathfrak{n}$, so ist $(\mathfrak{m}, \mathfrak{n}) = 1$, $(\mathfrak{n}, \mathfrak{m}) = m$.

§. 170.

Sind $\mathfrak{m}$, $\mathfrak{m}'$ zwei Moduln von der eben betrachteten Beschaffenheit, deren Zahlen μ, μ' demselben quadratischen Körper Ω angehören, so bilden alle Producte $\mu\mu'$ und deren Summen wieder einen solchen Modul $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$. Uebertragen wir die vorhergehenden Bezeichnungen durch Accentuation von $\mathfrak{m}$ auf $\mathfrak{m}'$ und $\mathfrak{m}''$, so müssen *erstens*, weil alle Producte $\mu\mu'$ in $\mathfrak{m}''$ enthalten sind, acht ganze rationale Zahlen $p, q \ldots p''', q'''$ existiren, welche den Gleichungen

$$\begin{aligned} \alpha\alpha' &= p\alpha'' + q\beta'' \\ \alpha\beta' &= p'\alpha'' + q'\beta'' \\ \beta\alpha' &= p''\alpha'' + q''\beta'' \\ \beta\beta' &= p'''\alpha'' + q'''\beta'' \end{aligned} \qquad (1)$$

*) Vergl. §. 161. Anm. — Ich erwähne hier nur noch Folgendes. Nennt man zwei Moduln $\mathfrak{a}$, $\mathfrak{b}$ verwandt, wenn $(\mathfrak{a}, \mathfrak{b})$ und $(\mathfrak{b}, \mathfrak{a})$ endlich sind, so sind zwei mit $\mathfrak{a}$ verwandte Moduln $\mathfrak{b}$, $\mathfrak{c}$ auch mit einander verwandt, und es ist

$$(\mathfrak{a}, \mathfrak{b})\,(\mathfrak{b}, \mathfrak{c})\,(\mathfrak{c}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})\,(\mathfrak{c}, \mathfrak{b})\,(\mathfrak{a}, \mathfrak{c}),$$

wovon man sich leicht durch die Betrachtung der kleinsten gemeinschaftlichen Vielfachen und grössten gemeinschaftlichen Theiler überzeugt.

genügen. Setzen wir zur Abkürzung*) die aus ihnen gebildeten partialen Determinanten

$$\begin{array}{l} pq'-qp'=P,\ \ pq''-qp''=Q,\ \ pq'''-qp'''=R,\\ p''q'''-q''p'''=U,\ \ p'q'''-q'p'''=T,\ \ p'q''-q'p''=S, \end{array} \quad (2)$$

so ist

$$RS=QT-PU, \quad (3)$$

und durch Elimination von α'', β'' aus je drei der Gleichungen (1) erhält man

$$\begin{array}{rl} * \quad U\alpha\beta'-T\beta\alpha'+S\beta\beta' &= 0\\ -U\alpha\alpha' \quad * \quad +R\beta\alpha'-Q\beta\beta' &= 0\\ T\alpha\alpha'-R\alpha\beta' \quad * \quad +P\beta\beta' &= 0\\ -S\alpha\alpha'+Q\alpha\beta'-P\beta\alpha' \quad * &= 0. \end{array} \quad (4)$$

Eliminirt man T aus der ersten und dritten, ferner U aus der ersten und zweiten dieser Gleichungen, so erhält man

$$P\beta^2-(R-S)\alpha\beta+U\alpha^2=0,$$
$$Q\beta'^2-(R+S)\alpha'\beta'+T\alpha'^2=0,$$

und folglich muss (zufolge (5) in §. 169)

$$\begin{array}{lll} P=an', & R-S=bn', & U=cn',\\ Q=a'n, & R+S=b'n, & T=c'n \end{array} \quad (5)$$

sein, wo n, n' ganze rationale, von Null verschiedene Zahlen bedeuten (denn n' muss eine ganze Zahl sein, weil a, b, c keinen gemeinschaftlichen Theiler haben, und wäre $n'=0$, also auch $P=0$, so wären α', β' zufolge (1) nicht unabhängig von einander); hierdurch nimmt die erste der Gleichungen (4) die Form

$$(b\beta-2c\alpha)\beta'n'=(b'\beta'-2c'\alpha')\beta n$$

an, mithin ist (zufolge (5) in §. 169)

$$n'\sqrt{d}=n\sqrt{d'}, \quad (6)$$

und hiermit sind die vier Gleichungen (4) vollständig befriedigt. Das Product dd' ist, wie zu erwarten war, eine Quadratzahl.

Da *zweitens* alle Zahlen μ'' des Moduls $\mathfrak{m}''$ durch Addition von Producten $\mu\mu'$ entstehen, so existiren acht ganze rationale Zahlen $u, v \ldots u''', v'''$, welche den Bedingungen

*) Die Bezeichnungen schliessen sich an die an, welche *Gauss* in den artt. 235, 236 der *Disquisitiones Arithmeticae* gewählt hat; die nothwendigen Modificationen sind leicht zu erkennen.

$$\begin{aligned} \alpha'' &= u\alpha\alpha' + u'\alpha\beta' + u''\beta\alpha' + u'''\beta\beta' \\ \beta'' &= v\alpha\alpha' + v'\alpha\beta' + v''\beta\alpha' + v'''\beta\beta' \end{aligned} \tag{7}$$

genügen. Substituirt man hierin die Gleichungen (1), und berücksichtigt, dass die Zahlen α'', β'' von einander unabhängig sind, so folgt

$$\begin{aligned} pu + p'u' + p''u'' + p'''u''' &= 1 \\ qu + q'u' + q''u'' + q'''u''' &= 0 \end{aligned} \tag{8}$$

und

$$\begin{aligned} pv + p'v' + p''v'' + p'''v''' &= 0 \\ qv + q'v' + q''v'' + q'''v''' &= 1. \end{aligned} \tag{9}$$

Bildet man die Determinante aus diesen vier Summen, so erhält man eine Gleichung von der Form

$$PP_1 + QQ_1 + RR_1 + SS_1 + TT_1 + UU_1 = 1, \tag{10}$$

wo die Determinanten $P_1 \ldots U_1$ auf dieselbe Weise aus den Zahlen $u, v \ldots u''', v'''$ gebildet sind, wie $P \ldots U$ aus $p, q \ldots p''', q'''$, und hieraus folgt, dass die sechs Zahlen (2) keinen gemeinschaftlichen Theiler haben. Dasselbe Resultat erhält man auch auf folgendem Wege; eliminirt man jede der vier Zahlen u, u', u'', u''' aus den beiden Gleichungen (8), so folgt

$$\begin{aligned} q &= \quad * \quad - Pu' - Qu'' - Ru''' \\ q' &= Pu \quad * \quad - Su'' - Tu''' \\ q'' &= Qu + Su' \quad * \quad - Uu''' \\ q''' &= Ru + Tu' + Uu'' \quad * \end{aligned} \tag{11}$$

ebenso erhält man aus (9) die Gleichungen

$$\begin{aligned} p &= \quad * \quad Pv' + Qv'' + Rv''' \\ p' &= -Pv \quad * \quad + Sv'' + Tv''' \\ p'' &= -Qv - Sv' \quad * \quad + Uv''' \\ p''' &= -Rv - Tv' - Uv'' \quad * \end{aligned} \tag{12}$$

Aus (11) folgt, dass jeder gemeinschaftliche Theiler der sechs Determinanten (2) in den vier Zahlen q, q', q'', q''', mithin zufolge (9) auch in der Zahl 1 aufgeht, was zu beweisen war. Hieraus ergiebt sich leicht mit Rücksicht auf (3), dass auch die sechs Zahlen (5) keinen gemeinschaftlichen Theiler haben; geht nämlich e in P, Q, $R - S$, $R + S$, T, U auf, so sind die Zahlen $2R$, $2S$ ebenfalls theilbar durch e, und die Quotienten $2R:e$ und $2S:e$ sind ent-

weder beide gerade oder beide ungerade, weil ihre Summe gerade ist; wären sie nun beide ungerade, so wäre auch ihr Product $4RS:e^2$ ungerade, was gegen die Gleichung (3) streitet, der zufolge RS durch e^2 theilbar ist; mithin sind R und S durch e theilbar, und folglich ist $e = \pm 1$. Es ergiebt sich daher, dass n und n' *relative Primzahlen* sind.

Durch Elimination der vier Zahlen α, β, α', β' aus den Gleichungen (1) erhält man

$$(p'\alpha'' + q'\beta'')(p''\alpha'' + q''\beta'') = (p\alpha'' + q\beta'')(p'''\alpha'' + q'''\beta'')$$

oder

$$L\beta''^2 - M\alpha''\beta'' + N\alpha''^2 = 0, \tag{13}$$

wenn man zur Abkürzung

$$\begin{gathered} q'q'' - qq''' = L, \quad p'p'' - pp''' = N, \\ pq''' + qp''' - p'q'' - q'p'' = M \end{gathered} \tag{14}$$

setzt. Wir zeigen zunächst, dass diese drei Zahlen durch nn' theilbar sind; da nämlich zufolge (5)

$$Q \equiv 0, \quad S \equiv -R, \quad T \equiv 0 \pmod{n}$$

ist, so ergiebt sich aus (11) und (12) in Bezug auf denselben Modul

$$\begin{aligned} q &\equiv -Pu' - Ru''', & p &\equiv Pv' + Rv''' \\ q' &\equiv Pu + Ru'', & p' &\equiv -Pv - Rv'' \\ q'' &\equiv -Ru' - Uu''', & p'' &\equiv Rv' + Uv''' \\ q''' &\equiv Ru + Uu'', & p''' &\equiv -Rv - Uv'' \end{aligned}$$

und hieraus

$$\begin{gathered} L \equiv (PU - R^2)(u'u'' - uu'''), \quad N \equiv (PU - R^2)(v'v'' - vv'''), \\ M \equiv (PU - R^2)(u'v'' + v'u'' - uv''' - vu'''); \end{gathered}$$

nun ist aber zufolge (3) $PU \equiv R^2 \pmod{n}$, folglich sind L, M, N theilbar durch n; da ferner auf dieselbe Weise sich zeigen lässt, dass sie auch durch n' theilbar sind, so müssen sie, weil n, n' relative Primzahlen sind, auch durch nn' theilbar sein; was zu beweisen war.

Führt man endlich die unabhängigen Variabeln x, y, x', y' und die bilinearen Functionen

$$\begin{aligned} x'' &= pxx' + p'xy' + p''yx' + p'''yy' \\ y'' &= qxx' + q'xy' + q''yx' + q'''yy' \end{aligned} \tag{15}$$

ein, so ergiebt sich durch Elimination von xx', xy', yx', yy'

$$\begin{array}{l} py'' - qx'' = \quad * \quad Pxy' + Qyx' + Ryy' \\ p'y'' - q'x'' = -Pxx' \quad * \quad + Syx' + Tyy' \\ p''y'' - q''x'' = -Qxx' - Sxy' \quad * \quad + Uyy' \\ p'''y'' - q'''x'' = -Rxx' - Txy' - Uyx' \quad * \end{array}$$

und hieraus folgt

$$\begin{array}{l} (p'y'' - q'x'')(p''y'' - q''x'') - (py'' - qx'')(p'''y'' - q'''x'') \\ = (Px^2 + (R - S)xy + Uy^2)(Qx'^2 + (R + S)x'y' + Ty'^2), \end{array} \tag{16}$$

d. h.

$$\begin{array}{l} Lx''^2 + Mx''y'' + Ny''^2 \\ = nn'(ax^2 + bxy + cy^2)(a'x'^2 + b'x'y' + c'y'^2). \end{array} \tag{17}$$

Da diese Gleichung eine Identität in Bezug auf die Variabeln x, y, x', y' wird, sobald x'', y'' durch die Ausdrücke (15) ersetzt werden, so muss, wenn enn' den grössten gemeinschaftlichen Divisor von L, M, N bedeutet, e in allen neun Producten $aa', ab' \ldots cc'$ aufgehen; diese letzteren haben aber keinen gemeinschaftlichen Theiler, weil dasselbe sowohl von den Zahlen a, b, c, wie von den Zahlen a', b', c' gilt; mithin ist $e = 1$, also *nn' der grösste gemeinschaftliche Theiler von L, M, N.* Nun ist ferner in Folge der bilinearen Substitution (15)

$$x''\alpha'' + y''\beta'' = (x\alpha + y\beta)(x'\alpha' + y'\beta'),$$

folglich auch

$$N(x''\alpha'' + y''\beta'') = N(x\alpha + y\beta)\, N(x'\alpha' + y'\beta'),$$

also

$$\begin{array}{c} m''(a''x''^2 + b''x''y'' + c''y''^2) = \\ mm'(ax^2 + bxy + cy^2)(a'x'^2 + b'x'y' + c'y'^2); \end{array}$$

mithin ergiebt sich durch Vergleichung mit (17)

$$nn'm''(a''x''^2 + b''x''y'' + c''y''^2) = mm'(Lx''^2 + Mx''y'' + Ny''^2);$$

diese Gleichung, welche eine Identität in Bezug auf die Variabeln x, y, x', y' wird, sobald x'', y'' durch die Ausdrücke (15) ersetzt werden, muss deshalb auch eine Identität in Bezug auf x'', y'' sein; da ferner m, m', m'' positiv sind, und die Zahlen a'', b'', c'' keinen gemeinschaftlichen Theiler haben, so ergiebt sich

$$m'' = mm' \tag{18}$$

und

$$L = a''nn', \quad M = b''nn', \quad N = c''nn', \tag{19}$$

also

$$a''x''^2 + b''x''y'' + c''y''^2 = (ax^2 + bxy + cy^2)(a'x'^2 + b'x'y' + c'y'^2). \quad (20)$$

Da endlich aus der Definition der Grössen (2) und (14), oder auch aus (16) sich leicht ergiebt, dass

$$M^2 - 4LN = (R-S)^2 - 4PU = (R+S)^2 - 4QT$$

ist, so folgt hieraus schliesslich

$$d''n^2n'^2 = dn'^2 = d'n^2,$$

d. h. die Determinante d'' ist der grösste gemeinschaftliche Theiler der beiden Determinanten

$$d = d''n^2, \quad d' = d''n'^2, \quad (21)$$

woraus sich leicht ergiebt, dass die Ordnung $\mathfrak{n}''$ des Productmoduls $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$ auch das Product $\mathfrak{n}\mathfrak{n}'$ aus den Ordnungen $\mathfrak{n}, \mathfrak{n}'$ von $\mathfrak{m}$, $\mathfrak{m}'$ ist. Ist ferner $\mathfrak{m}'$ das System $\mathfrak{o}$ aller ganzen Zahlen des Körpers Ω, so wird $\mathfrak{m}''$ ein Ideal im engeren Sinne des Wortes, nämlich der grösste gemeinschaftliche Theiler der beiden Ideale $\mathfrak{i}(\alpha)$, $\mathfrak{i}(\beta)$ oder aller Ideale $\mathfrak{i}(\mu)$; zugleich ist $m' = 1$, $m'' = m = N(\mathfrak{m}'')$, und $d' = d'' = \Delta(\Omega)$.

Wir stellen uns jetzt noch die Aufgabe, die Zahlen α'', β'' zu finden, wenn die Zahlen $\alpha, \beta, \alpha', \beta'$, also auch $a, b, c, \sqrt{d}, a', b', c', \sqrt{d'}$ gegeben sind; die nachfolgende Lösung ist, abgesehen von geringfügigen Aenderungen, der eleganten Methode entlehnt, welche von *Gauss* zu ähnlichem Zweck angewandt ist und sich in hohem Grade verallgemeinern lässt (vergl. §. 161, Anm.). Die beiden relativen Primzahlen n, n' sind durch (6), und folglich die sechs ganzen Zahlen $P \dots U$ durch (5) (bis auf einen gemeinschaftlichen Factor ± 1) aus den Daten vollständig bestimmt, und zwar so, dass sie die Gleichungen (3), (4) befriedigen und keinen gemeinschaftlichen Theiler haben*). Nun wähle man, durch die Gleichungen (11) geleitet, vier ganze rationale Zahlen $\mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}''$, $\mathfrak{Q}'''$ willkürlich, nur mit der einzigen Beschränkung, dass die folgenden vier Zahlen

*) Dass R und S (zufolge (5)) *ganze* Zahlen werden und keinen gemeinschaftlichen Theiler mit P, Q, T, U haben, geht unmittelbar aus der Gewissheit hervor, dass der Modul $\mathfrak{m}''$ und die Basiszahlen α'', β'' *existiren*; es lässt sich aber auch sehr leicht aus (5) und (6) beweisen, natürlich unter der Voraussetzung, dass dd' eine Quadratzahl ist.

$$\begin{array}{rrrrl} * & P\mathfrak{Q}' & +Q\mathfrak{Q}'' & +R\mathfrak{Q}''' & = rq \\ -P\mathfrak{Q} & * & +S\mathfrak{Q}'' & +T\mathfrak{Q}''' & = rq' \\ -Q\mathfrak{Q} & -S\mathfrak{Q}' & * & +U\mathfrak{Q}''' & = rq'' \\ -R\mathfrak{Q} & -T\mathfrak{Q}' & -U\mathfrak{Q}'' & * & = rq''' \end{array} \quad (22)$$

nicht sämmtlich verschwinden und folglich einen grössten gemeinschaftlichen Divisor r besitzen; nachdem hierdurch vier ganze Zahlen q, q', q'', q''' ohne gemeinschaftlichen Theiler gewonnen sind, wähle man (nach §. 24) vier ganze rationale Zahlen v, v', v'', v''' so, dass

$$qv + q'v' + q''v'' + q'''v''' = 1 \quad (23)$$

wird, und bestimme die Zahlen p, p', p'', p''' durch die Gleichungen (12); endlich wähle man sechs ganze rationale Zahlen P', Q', R', S', T', U' (nach §. 24) so, dass

$$PP' + QQ' + RR' + SS' + TT' + UU' = 1 \quad (24)$$

wird, setze hierauf

$$\begin{array}{rl} u = & * \quad P'q' + Q'q'' + R'q''' \\ u' = & -P'q \quad * \quad + S'q'' + T'q''' \\ u'' = & -Q'q - S'q' \quad * \quad + U'q''' \\ u''' = & -R'q - T'q' - U'q'' \quad * \end{array} \quad (25)$$

und bestimme die Zahlen α'', β'' durch die Gleichungen (7), so bilden dieselben eine Basis des Moduls $\mathfrak{m}''$, d. h. sie genügen den Gleichungen (1).

Um sich hiervon zu überzeugen, bemerke man zunächst, dass aus (22) mit Rücksicht auf (3) die Relationen

$$\begin{array}{rrrrl} * & Uq' & -Tq'' & +Sq''' & = 0 \\ -Uq & * & +Rq'' & -Qq''' & = 0 \\ Tq & -Rq' & * & +Pq''' & = 0 \\ -Sq & +Qq' & -Pq'' & * & = 0 \end{array}$$

folgen; mit Hülfe derselben ergiebt sich aus (12) und (23)

$$\begin{aligned} pq' - qp' &= (Pv' + Qv'' + Rv''')q' - (-Pv + Sv'' + Tv''')q \\ &= P(qv + q'v') + (Qq' - Sq)v'' + (Rq' - Tq)v''' \\ &= P(qv + q'v' + q''v'' + q'''v''') = P, \end{aligned}$$

und auf ähnliche Weise erhält man die fünf anderen Gleichungen (2). Mithin folgt die erste der beiden Gleichungen (8), wenn man die Gleichungen (25) mit p, p', p'', p''' multiplicirt und mit Rück-

sicht auf (24) addirt; die zweite Gleichung (8) ergiebt sich unmittelbar aus (25), wenn man mit q, q', q'', q''' multiplicirt und addirt. Es gelten daher auch die aus (8) und (2) abgeleiteten Gleichungen (11). Von den Gleichungen (9) findet die zweite zufolge (23) Statt, während die erste sich aus (12) ergiebt, wenn man mit v, v', v'', v''' multiplicirt und addirt. Setzt man ferner zur Abkürzung

$$uv' - vu' = P_1, \quad uv'' - vu'' = Q_1, \quad uv''' - vu''' = R_1,$$
$$u''v''' - v''u''' = U_1, \quad u'v''' - v'u''' = T_1, \quad u'v'' - v'u'' = S_1,$$

so ergiebt sich die Gleichung (10) entweder auf die dort angegebene Weise aus (8) und (9), oder auch aus (12), wenn man mit u, u', u'', u''' multiplicirt und unter Rücksicht auf (8) addirt. Substituirt man ferner für p, q ihre Ausdrücke aus (12) und (11), so erhält man

$$\begin{aligned} pu\ + qv &= PP_1 + QQ_1 + RR_1 \\ pu' + qv' &= QS_1 + RT_1 \\ pu'' + qv'' &= -PS_1 + RU_1 \\ pu''' + qv''' &= -PT_1 - QU_1. \end{aligned}$$

Multiplicirt man diese Gleichungen mit $\alpha\alpha', \alpha\beta', \beta\alpha', \beta\beta'$ und addirt, so folgt aus den Definitionen (7) mit Rücksicht auf (4) und (10) die erste der Gleichungen (1); da die anderen sich auf ganz ähnliche Art ergeben, so bilden die durch die Gleichungen (7) definirten Zahlen α'', β'' in der That eine Basis des Productes $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$, was zu beweisen war.

Wir bemerken zum Schluss, dass man für die ersten Basiszahlen $\alpha, \alpha', \alpha''$ stets die kleinsten positiven ganzen rationalen Zahlen g, g', g'' wählen kann, welche in den Moduln $\mathfrak{m}, \mathfrak{m}', \mathfrak{m}''$ enthalten sind; dann wird $q = 0$, und die Bestimmung von $\mathfrak{m}''$ aus $\mathfrak{m}$ und $\mathfrak{m}'$ lässt sich auf ein System von Congruenzen reduciren, ähnlich wie in dem speciellen Falle, welcher in den §§. 145, 146 behandelt ist*).

*) Vergl. *Arndt: Auflösung einer Aufgabe in der Composition der quadratischen Formen.* Crelle's Journal LVI.

Druckfehler.

Seite 109, Zeile 1 ist zu lesen $\left(\frac{11}{365}\right) = \left(\frac{365}{11}\right) = \left(\frac{2}{11}\right) = -1$.
Seite 157, Zeile 15 ist ψ' statt ψ zu lesen.
Seite 226, Zeile 18 ist *Zahl* statt *Zahlen* zu lesen.

Häusler.

1. 4

